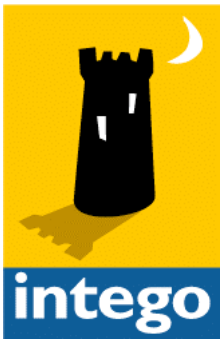
# Benutzerhandbuch



**Intego VirusBarrier X für Macintosh**

Copyright © 2000 bis 2002 by Intego, Inc. Alle Rechte vorbehalten.

Intego, Inc.

www.intego.com

Dieses Handbuch enthält die Bedienungsanleitung für die Antivirussoftware Intego VirusBarrier X für Macintosh. Dieses Handbuch und die Antivirussoftware Intego VirusBarrier X sind urheberrechtlich geschützt. Alle Rechte vorbehalten. Dieses Handbuch und die Antivirussoftware Intego VirusBarrier X dürfen nur reproduziert werden, wenn dies in der zugehörigen Softwarelizenzvereinbarung oder schriftlich von Intego, Inc. genehmigt wurde.

Eigentumsrechte an der Software haben ausschließlich Intego und seine Vorlieferanten. Die Struktur, die Organisation sowie der Quell- und Maschinencode der Software sind Geschäftsgeheimnisse von Intego und seinen Vorlieferanten. Die Software unterliegt US-amerikanischem und internationalem Urheberrecht.

Intego VirusBarrier X verwendet die von Erik Dörnenburg entwickelten Grundstrukturen EDCommon und EDInternet.

## Inhaltsverzeichnis


*1- Über Intego VirusBarrier X* ..... *4*

**Was ist Intego VirusBarrier X?** ..... **5**

**Die Eigenschaften von Intego VirusBarrier X** ..... **8**

**Über dieses Benutzerhandbuch** ..... **10**

*2 - Einführung in die Welt der Computerviren* ..... *12*

**Weshalb Ihr Macintosh unbedingt vor Viren geschützt werden sollte** ..... **13**

**Was ist ein Computervirus?** ..... **14**

Wer entwickelt Viren? ..... 16

Wie Viren funktionieren ..... 17

**Die unterschiedlichen Arten von Viren** ..... **20**

Systemviren ..... 21

Dateiviren ..... 24

Falsche Viruswarnungen ..... 29

Wie verbreiten sich Computerviren? ..... 30

Wie können Sie Ihren Macintosh vor Viren schützen? ..... 32

*3 - Installation* ..... *35*

**Systemanforderungen** ..... **36**

**Installieren von Intego VirusBarrier X** ..... **36**

**Registrieren von Intego VirusBarrier X** ..... **41**

**Verwenden von Intego VirusBarrier X im Demonstrationsmodus** ..... **42**

*4 - Erste Schritte* ..... *43*

**Der Standardmodus von Intego VirusBarrier X** ..... **44**

Bedienungsoberfläche von Intego VirusBarrier X ..... 44

**Manuelles Starten einer Virensuche** ..... **46**

**Voreinstellungen von NetUpdate** ..... **49**

**Virensuche mit Ziehen und Ablegen** ..... **52**

**Verwenden von Intego VirusBarrier X im Dock** ..... **52**

***5 - Funktionen von Intego VirusBarrier X*** ..... ***55***

**Virensuche** ..... **56**

Manuell gestartete Virensuche ..... 56

Virensuche mit Ziehen und Ablegen ..... 65

Ergebnisse der Virensuche ..... 65

**Warnmeldungen** ..... **70**

***6 - Einstellungen von Intego VirusBarrier X*** ..... ***72***

**Voreinstellungen** ..... **73**

Optionen für die Alarmierung ..... 80

**NetUpdate** ..... **82**

Virenbeschreibung ..... 84

**Über Intego VirusBarrier X** ..... **85**

***7 - Diagnose*** ..... ***87***

**Wenn Sie vermuten, dass Ihr Macintosh mit einem Virus infiziert ist** ..... **88**

**Prinzipielle Vorsichtsmaßnahmen** ..... **90**

***8 - Technische Kundenunterstützung*** ..... ***92***

***9 - Anhang*** ..... ***94***

**Häufig verwendete Fachbegriffe** ..... **95**

**Virenbeschreibung** ..... **99**

# 1- Über Intego VirusBarrier X

# Was ist Intego VirusBarrier X?

Intego VirusBarrier X ist eine einfach zu bedienende, schnelle und transparente Antiviruslösung für Macintosh-Computer von Intego, dem Hersteller der weithin als erstklassig anerkannten Sicherheitssoftware NetBarrier. Intego VirusBarrier X schützt Ihren Macintosh vor Computerviren aller Art. Diese können in Dateien, Anwendungsprogrammen auf Disketten, CD-ROMs, anderen Wechseldatenträgern und in aus dem Internet oder einem Netzwerk geladenen Dateien enthalten sein.

Intego VirusBarrier X schützt Ihren Macintosh vor Viren, indem alle von Ihrem Macintosh gelesenen und geschriebene Dateien überwacht werden. Ferner überwacht das Antivirusprogramm Ihren Macintosh auf verdächtige Aktivitäten, die darauf hindeuten, dass ein Virus ein Anwendungsprogramm oder eine andere Datei verfälscht. Wenn Sie Intego VirusBarrier X auf Ihrem Macintosh installiert haben, können Sie sicher sein, dass Ihr Macintosh optimal vor allen Viren geschützt ist.

Intego VirusBarrier X ist ein Anwendungsprogramm, das im Hintergrund läuft, sämtliche Aktivitäten Ihres Macintosh überwacht und alle an Ihren Macintosh angeschlossenen Datenträger nach Viren durchsucht. Intego VirusBarrier X kennt die Signaturen (spezifische Bitmuster) aller Macintosh-Viren. Wenn ein neues Macintosh-Virus auftaucht, werden die Virendefinitionen sofort vom Antivirus-Softwareentwicklungsteam von Intego aktualisiert, die mit Hilfe der einzigartigen Funktion NetUpdate von Intego VirusBarrier X automatisch heruntergeladen werden.

Gleichzeitig mit dem Kauf von Intego VirusBarrier X erwerben Sie ein kostenloses Abonnement auf alle Aktualisierungen der Virendefinitionen über 1 (ein) Jahr. Nach Ablauf dieser Zeit können Sie auf der Intego-Website www.intego.com oder mit Hilfe der Funktion NetUpdate ein weiteres Abonnement bestellen.

Intego VirusBarrier X wurde unter Berücksichtigung spezieller Kriterien entwickelt. Die prinzipielle Vision der Softwareentwickler bei Intego war, eine Antivirussoftware zu entwickeln, die vollautomatisch arbeitet: nach der Installation und Konfiguration der Software sollte der Macintosh-Benutzer sich in Bezug auf Viren um nichts mehr kümmern müssen, es sei denn, dass die Antivirussoftware einen Virenbefall erkannt hat. Die hinter Intego VirusBarrier X stehende Philosophie lässt sich in drei Wörtern verdeutlichen: **Einfach**, **schnell** und absolut **unaufdringlich**.

## Einfach

Intego VirusBarrier X ist die am einfachsten zu bedienende Antivirussoftware. Nach der Installation arbeitet die Software im Hintergrund, beobachtet jede Aktivität Ihres Macintosh und prüft Ihre Dateien auf Virenbefall, ohne dass Sie überhaupt etwas davon merken.

## Schnell

Intego VirusBarrier X ist schnell und effizient. Intego VirusBarrier X beeinträchtigt die Arbeitsgeschwindigkeit Ihres Macintosh nicht im Geringsten. Nach der Installation und Konfiguration der Software ist kein weiterer manueller Eingriff erforderlich. Bei jedem Schreiben oder Lesen einer Datei

wird diese von Intego VirusBarrier X daraufhin geprüft, ob sie von einem Virus befallen wurde.

## Unaufdringlich

Intego VirusBarrier X ist vollkommen absolut unaufdringlich. Im Gegensatz zu vielen anderen Antivirusprogrammen werden Sie beim Installieren von Software nicht ständig über "verdächtige" Aktivitäten alarmiert. Fehlalarme gehören ebenfalls der Vergangenheit an. Nach der Installation von Intego VirusBarrier X werden Sie höchstwahrscheinlich vergessen, dass Sie überhaupt eine Antivirussoftware installiert haben. Sie werden sich erst dann wieder an die Existenz von Intego VirusBarrier X erinnern, wenn die Software ein Virus erkannt hat und eine entsprechende Warnmeldung ausgibt. Im Gegensatz zu vielen anderen Antivirusprogrammen ist es bei Intego VirusBarrier X nicht notwendig, dieses vor der Installation neuer Anwendungssoftware abzuschalten, auch wenn im Handbuch oder im Installationsprogramm der neuen Software eigens darauf hingewiesen wird. Intego VirusBarrier X kann jederzeit im Hintergrund laufen und schützt hierbei Ihren Macintosh, ohne dass Sie selbst jemals manuell eingreifen müssen.

# Die Eigenschaften von Intego VirusBarrier X

### Virensuche

Intego VirusBarrier X kann in unterschiedlichen Betriebsarten arbeiten. Während die Antivirussoftware Ihren Macintosh kontinuierlich überwacht und dadurch vor Virenbefall schützt, können Sie die Software auch manuell bedienen, um beispielsweise eine Festplatte oder einen Datenträger im Netzwerk auf Viren durchsuchen zu lassen.

### Automatische Reparatur

Wenn Intego VirusBarrier X im Automatikmodus arbeitet, wird jede von einem Virus infizierte Datei automatisch repariert, indem das Virus aus der Datei gelöscht wird. Wenn dies nicht möglich ist, gibt die Antivirussoftware eine Meldung aus, in der Sie darauf hingewiesen werden, dass die betreffende Datei beschädigt ist. In diesem Modus müssen Sie sich nicht um die Aktivitäten von Intego VirusBarrier X kümmern - die Software tritt erst dann in Aktion, wenn sie ein Virus oder eine andere verdächtige Datei gefunden hat.

### Manuelle Virensuche

Sie können eine Virensuche auch manuell starten. Dies sollten Sie unmittelbar nach der Installation von Intego VirusBarrier X tun, um sicherzustellen, dass Ihr Macintosh nicht von Viren befallen ist. Selbstverständlich können Sie die manuelle Virensuche auch zu jedem späteren Zeitpunkt starten, um Datenträger nach Viren zu durchsuchen.

**Turbomodus**

Im Turbomodus wird die Virensuche erheblich beschleunigt. Beim erstmaligen Durchsuchen eines Datenträgers "merkt" sich Intego VirusBarrier X, welche Dateien auf Viren durchsucht wurden. Wenn diese Dateien zwischenzeitlich nicht verändert wurden, so werden sie von Intego VirusBarrier X nicht durchsucht, sodass die Virensuche ca. 5- bis 40-mal schneller durchgeführt wird.

**Protokolle**

Intego VirusBarrier X protokolliert jedes gefundene Virus sowie jede gefundene verdächtige Datei. Sie können diese Protokolle prüfen, um zu sehen, ob Dateien oder Anwendungsprogramme infiziert, repariert oder beschädigt wurden.

**Dock**

Wenn Sie das Symbol von Intego VirusBarrier X im Dock von Mac OS X anzeigen lassen, können Sie Dateien oder den Inhalt eines Ordners auf einfachste Weise nach Viren durchsuchen lassen, indem Sie die Dateien oder den Ordner aufs Symbol von Intego VirusBarrier X im Dock von Mac OS X ziehen.

**NetUpdate**

Mit dem Softwarepaket Intego VirusBarrier X wird das einzigartige Aktualisierungsprogramm NetUpdate geliefert, mit dem Sie prüfen können, ob es neue Versionen von Intego VirusBarrier X oder neue Virendefinitionen gibt. Diese Prüfung kann automatisch oder manuell durchgeführt werden. Wenn die Aktualisierungsfunktion automatisch

ausgeführt werden soll, müssen Sie lediglich das Zeitintervall festlegen, in dem auf neue Versionen von Intego VirusBarrier X oder auf neue Virendefinitionen geprüft werden soll. Sie können beispielsweise festlegen, dass NetUpdate an einem bestimmten Wochentag zu einer bestimmten Uhrzeit oder in Abständen von jeweils einer Woche gestartet werden soll. Wenn Sie die Aktualisierung lieber manuell durchführen wollen, genügt ein einziger Mausklick, um eine Verbindung mit dem Intego-Server herzustellen und zu prüfen, ob eine neue Version von Intego VirusBarrier X oder neue Virendefinitionen zur Verfügung stehen.

**Virusmeldungen**

Intego VirusBarrier X ermöglicht es Ihnen, festzulegen, wie Sie über erkannte Viren alarmiert werden, während die Antivirussoftware im Hintergrund läuft. Sie können festlegen, dass bei Erkennung eines Virus ein Fenster mit einer Warnmeldung erscheint, ein akustischer Alarm ertönt oder eine e-Mail-Mitteilung an eine bestimmte e-Mail-Adresse gesandt wird. Die letztgenannte Funktion ist besonders dann von großem Nutzen, wenn Intego VirusBarrier X auf Macintosh-Computern läuft, die mit einem Netzwerk verbunden sind, und ein Netzwerkverwalter oder der Besitzer des entsprechenden Macintosh alarmiert werden soll.

## Über dieses Benutzerhandbuch

Dieses Benutzerhandbuch enthält detaillierte Informationen über die Installation, die Verwendung und die Aktualisierung von Intego VirusBarrier X

sowie eine vollständige Beschreibung aller Macintosh-Viren und ein Glossar mit Begriffen aus der Welt der Viren.

Am Besten lesen Sie zunächst die Einführung durch, um zu erfahren, worum es sich bei Viren eigentlich handelt. Gehen Sie dann gemäß den Installationshinweisen im Kapitel 3 vor. Als nächstes sollten Sie die Beschreibung der Funktionen von Intego VirusBarrier X im Kapitel 5 durchlesen. Wenn Sie noch mehr über Viren wissen wollen, empfiehlt sich die Lektüre der Virenbeschreibung und des Glossars im Kapitel 9.

Wenn Sie einmal Probleme mit Ihrem Macintosh haben und vermuten, dass die Störung durch ein Virus verursacht wurde, sollten Sie den Abschnitt "Diagnose" im Kapitel 7 durchlesen. Dort finden Sie Hinweise zur Fehlersuche an Ihrem Macintosh und dazu, ob Ihr Macintosh wirklich von einem Virus befallen ist. Falls ja, befolgen Sie bitte die Anweisungen in Bezug auf das Einsenden der Dateien ans Virus Monitoring Center von Intego, die Ihrer Meinung nach von Viren befallen sind, sodass die Viren von unseren Experten geprüft werden können.

# 2 - Einführung in die Welt der Computerviren

## Weshalb Ihr Macintosh unbedingt vor Viren geschützt werden sollte

Sie wissen sehr gut, dass auf den Datenträgern Ihres Macintosh wichtige Informationen gespeichert sind. Sie verwenden Ihren Macintosh für Ihre Arbeit oder Ihre privaten Hobbys, und wissen, wie viel Zeit und unter Umständen auch Geld es kosten würde, verloren gegangene Dateien zu ersetzen. Selbst wenn Sie Ihren Macintosh nur zuhause im privaten Bereich einsetzen, haben auch Sie bestimmt Dateien gespeichert, die Sie nur äußerst ungern verlieren würden. Wenn ein Virus alle Ihre Dateien zerstören oder löschen würde, müssten Sie selbst viel Zeit in die Neuinstallation Ihres Betriebssystems und Ihrer Anwendungssoftware sowie in die Konfiguration Ihres Computersystems investieren.

Ein gutes Antivirusprogramm ist wie eine gute Versicherung. Selbstverständlich hoffen Sie, dass Ihnen mit Ihrem Macintosh niemals ein Missgeschick passieren wird, doch falls dies doch einmal geschehen sollte, würde Ihnen das bestimmt einigen Ärger bereiten. Intego VirusBarrier X ist Ihre persönliche Versicherung gegen alle Arten von Viren, indem diese Antivirussoftware Ihren Macintosh kontinuierlich auf Virenbefall überwacht.

Die Bedrohung durch Viren ist Realität. Jeden Tag werden immer mehr neue Viren entdeckt. Obwohl Sie als Besitzer eines Macintosh im Vergleich mit einem PC-Benutzer nur mit einer relativ geringen Wahrscheinlichkeit damit rechnen müssen, dass Ihr Macintosh von Viren infiziert wird, ist diese Gefahr

selbstverständlich immer existent, was zur Folge hätte, dass Ihre Dateien beschädigt oder unbrauchbar werden.

## Was ist ein Computervirus?

Nichts kann einen Computerbenutzer mehr schockieren, als wenn er den Verdacht hat, dass sein Computer mit einem Virus infiziert ist. In vielen Fällen reagieren Computerbenutzer so, als seien sie persönlich von einem (biologischen) Virus infiziert worden. Fast jeder Computerbenutzer hat bereits Gräuelgeschichten von Viren gehört oder gelesen, aus denen hervorgeht, welche Schäden Viren an Computersystemen anrichten können. Manche Computerbenutzer geraten zwar nicht so sehr in Panik, aber keinen Computerbenutzer wird es vollkommen gleichgültig lassen, wenn er erfährt, dass sein Computersystem mit einem Virus infiziert ist.
Der Befall von Computersystemen mit Viren ist heute, in einer durch und durch vernetzten Welt, weitaus eher wahrscheinlich als noch vor wenigen Jahren. Einer der Hauptgründe für das große Risiko eines Befalls mit Viren ist der heutzutage sehr rege e-Mail-Verkehr. Ein Virus kann sich so schnell wie eine epidemische Grippe verbreiten. Doch nun: Was sind eigentlich Viren? Welche Funktion haben sie? Weshalb sind sie so gefährlich?

Der Begriff "Virus" wurde erstmals in den frühen 80er Jahren des 20. Jahrhunderts im Zusammenhang mit Computern verwendet. Hiermit bezeichnete man Computerprogramme, die sich selbst vervielfältigen können.

Ein Virus ist nichts anderes als ein ablauffähiges Computerprogramm, das in eine Datei oder ein Anwendungsprogramm eingebettet ist. Viren werden über Disketten, CD-ROMs, andere Datenträger oder übers Internet verbreitet. Wie biologische Viren, von denen Lebewesen befallen werden, versuchen auch Computerviren, sich zu reproduzieren. Viren betten sich dabei in weitere Dateien und Anwendungsprogramme ein. Viren erzeugen identische Kopien von sich selbst, infizieren die Datenträger anderer Computer, usw.

Computerviren sind nichts anderes als kleine Computerprogramme. Je kleiner sie sind, umso besser können sie sich unbemerkt in Dateien und Anwendungsprogramme einbetten. Viren wurden nur zu einem einzigen Zweck entwickelt: Um sich zu vermehren und immer mehr Computersysteme zu befallen. Einige Viren sind unschädlich, sondern bewirken lediglich das Öffnen eines Fensters mit einer Meldung auf dem Bildschirm, während andere Dateien beschädigen, zerstören oder löschen. Einige Viren wurde ohne jede böse Absicht entwickelt, während die meisten die einzige Aufgabe haben, Dateien zu beschädigen und andere Computersysteme zu befallen.

Viren können jeden Computer - Ihren Macintosh zuhause oder alle Computer eines Unternehmensnetzwerks - infizieren, sofern keine Vorsichtsmaßnahmen getroffen werden. Die beste Möglichkeit, einen Macintosh vor Viren zu schützen, ist die Verwendung von Intego VirusBarrier X, und dafür Sorge zu tragen, dass dieses Antivirusprogramm und die Virendefinitionen jederzeit aktuell sind.

## Wer entwickelt Viren?

Im Gegensatz zum weit verbreiteten Gerücht werden Viren nicht von den Softwareherstellern entwickelt, die Antivirusprogramme verkaufen. Diese Softwarehersteller haben genug damit zu tun, ihre Antivirusprogramme stets auf dem neuesten Stand zu halten, um ihren Kunden auch gegen die neuesten Viren ein wirksames Gegenmittel anbieten zu können.

Niemand weiß genau, wer Viren entwickelt. Sind es unzufriedene Teenager oder geschickte Hacker? Niemand weiß es genau. Bisher wurden einige wenige Entwickler von Viren verhaftet, aber die meisten bleiben unentdeckt. Die Virenentwickler, die man bisher erwischte, wollten vielleicht sogar erkannt werden, um Aufmerksamkeit auf sich zu ziehen. Immerhin wurden bereits Viren entdeckt, die den Namen ihres Entwicklers enthielten. Andere Entwickler von Viren sind nichts anderes als Vandalen, die einfach ihren Spaß daran haben, wenn sie sehen, welche Schäden sie mit ihren relativ simpel gestrickten Machwerken angerichtet haben. Andere wiederum sind nur neugierig, zu erfahren, wie weit sich ihre Produkte verbreiten. Wie einmal jemand sagte, sind Viren aber vielleicht auch nichts anderes als "die elektronische Form von Graffiti".

In vielen Fällen wurden Computerviren ohne böse Absichten programmiert, verursachen aber trotzdem viele Probleme. Ein Beispiel hierfür ist das Virus MacMag, dessen Aufgabe darin bestand, weltweit eine Friedensbotschaft zu verbreiten. Eine genauere Beschreibung dieses Virus finden Sie im Kapitel 9.

Seitdem nahezu jeder Benutzer eines Computers gleichzeitig auch Internet-Benutzer ist, besteht nicht nur die Gefahr, dass ein geistig Verwirrter Viren programmiert, um Aufmerksamkeit zu erlangen und sich dadurch aus seiner Isolation zu befreien. Viel gefährlicher sind Programmierer, die Viren produzieren, um absichtlich große wirtschaftliche Schäden anzurichten. Die weite Verbreitung von Viren wie z.B. von LoveBug verdeutlichte, welche materiellen Schäden ein Unternehmen infolge von Produktionseinbußen und Stillstandszeiten erleiden kann, wenn seine Computer von einem Virus befallen werden. Schon allein aus diesem Grund sollten Sie Ihren Macintosh so gut vor Viren schützen, wie dies überhaupt möglich ist.

## Wie Viren funktionieren

Die meisten Computerbenutzer missverstehen unter einem Virus jede Software, die zu dem Zweck entwickelt wurde, Schäden zu verursachen. Allerdings hat ein Großteil dieser schädlichen Software nichts mit einem Virus zu tun: Beispielsweise funktionieren Trojanische Pferde (umgangssprachlich: "Trojaner") und Würmer anders als Viren und vermehren sich nicht wie Viren. Die meisten Computerbenutzer zählen diese schädlichen Programme jedoch zu den Viren. Obwohl diese Software schädlich ist und die Dateien auf den Datenträgern eines Computers beschädigen, zerstören oder löschen können, funktionieren Trojanische Pferde, Würmer und dergleichen anders als Viren.

Ein echtes Virus ist Maschinencode (unmittelbar ausführbarer Programmcode), der auf einem Zielcomputersystem ausgeführt werden kann. Aus diesem Grund sind Viren, die für PCs mit dem Betriebssystem Windows oder MS-DOS

entwickelt wurden, für Macintosh-Computer vollkommen unschädlich. Dies gilt selbstverständlich auch umgekehrt. (Eine Ausnahme hiervon gilt jedoch dann, wenn Sie beispielsweise einen Windows-Emulator auf Ihrem Macintosh laufen lassen. In diesem Fall kann das emulierte Windows-System von einem Windows-Virus beschädigt werden.)

Viren führen zwei Operationen aus, nachdem sie ein Computersystem befallen haben. Zuerst wird der Virenprogrammcode ausgeführt, der dafür vorgesehen ist, das betreffende Computersystem zu schädigen. Anschließend reproduziert sich das Virus selbst, indem es sich in andere Dateien und Anwendungsprogramme sowie auf an den Computer angeschlossene Datenträger kopiert. Anhand des nachstehenden Beispiels wird erklärt, wie ein fiktives Virus Ihren Macintosh schädigen könnte. (Eigentlich handelt es sich beim nun beschrieben Virus um ein Trojanisches Pferd, da dessen Funktionsweise einfacher verständlich ist.)

> Ein Freund oder Kunde schickt Ihnen übers Internet ein mit einem Virus infiziertes Programm. Obwohl Sie wissen, dass Sie e-Mail-Anhänge von Unbekannten nicht öffnen sollten, öffnen Sie die e-Mail-Mitteilung und dann den darin enthaltenen Anhang. Schließlich kam die e-Mail-Mitteilung von einer Person Ihres Vertrauens. Bei diesem Anhang handelt es sich um ein Programm, beispielsweise um eine selbstlaufende animierte Grußkarte. Sie doppelklicken aufs Symbol dieses Anhangs, sodass das Programm gestartet wird. Während des Programmlaufs wird der darin enthaltene schädliche Programmcode in die Systemdatei auf dem Systemdatenträger Ihres Macintosh kopiert. Gleichzeitig wird das Netzwerk Ihres Unternehmens nach anderen Macintosh-Computern

durchsucht, in deren Systemdateien der schädliche Programmcode ebenfalls kopiert wird. Nachdem die Animation in der Grußkarte abgespielt wurde, beenden Sie dieses Programm. Ihrem Macintosh geschieht nun noch nichts, da der Viruscode erst nach einem Neustart Ihres Computersystems in Aktion tritt.

Am nächsten Morgen kommen Sie in Ihr Büro, starten Ihren Macintosh und stellen fest, dass der Startvorgang ungewöhnlich lang dauert. Nachdem das Betriebssystem Ihres Macintosh endlich gestartet ist, stellen Sie fest, dass Ihr Macintosh sehr langsam arbeitet. Wenn Sie den Bericht öffnen wollen, den Sie bis zur Mittagszeit fertig stellen müssen, erkennen Sie, dass dieser Bericht gar nicht mehr auf der Festplatte Ihres Macintosh vorhanden ist. Sie wechseln in den Finder und durchsuchen nun die interne Festplatte Ihres Macintosh. Hierbei stellen Sie fest, dass Dutzende oder gar Hunderte Ihrer Dateien fehlen. Erst jetzt durchzuckt Sie der Gedanke, dass Sie gestern vergessen hatten, eine Datensicherung aller Ihrer Dateien durchzuführen, sodass Sie über keine Sicherungskopien der fehlenden Dateien verfügen.

Zwischenzeitlich haben Sie die animierte Grußkarte an mehrere Ihrer Freunde und Bekannten versandt, wissen aber zu diesem Zeitpunkt immer noch nicht, dass das Fehlen Ihrer Dateien mit dieser animierten Grußkarte zu tun hat. Einige Stunden später erhalten Sie einen Anruf von einem Ihrer Freunde, der Ihnen erklärt, dass die animierte Grußkarte sein Computersystem beschädigte.

Wie Sie sehen, kann ein Virus beträchtlichen Schaden verursachen. Und zwar nicht nur bei Ihnen, sondern auch bei anderen Personen, mit denen Sie in Verbindung stehen. Eines der größten Probleme mit Viren ist heute, dass die meisten Computerbenutzer täglich viele e-Mail-Mitteilungen versenden, sodass Computersysteme weitaus schneller als noch vor wenigen Jahren infiziert werden können, als Dateien noch durch den Austausch von Disketten verteilt wurden. Indem Sie Ihren Macintosh mit Intego VirusBarrier X vor einem Befall mit Viren schützen, tun Sie dies auch indirekt mit den Computersystemen anderer Personen.

Jeder, der sich mit aktuellen Geschehnissen in der Welt befasst, weiß, dass es in letzter Zeit Viren gab, die sich innerhalb von weniger als 24 Stunden über die gesamte Erde verbreitet haben. Obwohl diese besonders schädlichen Viren wie z.B. Melissa und der Wurm Love Bug nur PCs infizieren, auf denen das Betriebssystem Windows läuft, ist zu befürchten, dass derart schädliche Viren eines Tages auch für den Macintosh programmiert werden.

## Die unterschiedlichen Arten von Viren

Viren lassen sich zwei unterschiedlichen Kategorien zuordnen. Dies hängt davon ab, was vom jeweiligen Virus attackiert wird. Die eine Kategorie von Macintosh-Viren wird als Systemvirus bezeichnet, da diese Viren die Systemdatei, Systemerweiterungen oder die Schreibtischdateien infizieren. Die Macintosh-Viren der zweiten Kategorie werden als Dateiviren bezeichnet. Sie attackieren Anwendungsprogramme, Datendateien, Kontrollfelder und Systemerweiterungen.

## Systemviren

Systemviren sind die gefährlichsten Macintosh-Viren, da sie das Betriebssystem beschädigen. In diesem Abschnitt beschreiben wir auch zwei andere Arten "bösartiger" Software: Trojanische Pferde und Würmer. Obwohl die schädliche Software dieses Typs technisch anders als "echte" Viren funktioniert, wirkt sie sich allgemeiner als Dateiviren aus.

## Viren

Ein Virus ist ein kleines Programm, das wie ein Parasit wirkt und sich in einem Wirtsprogramm oder einer Wirtsdatei einnistet. Das Virus infiziert Dateien und Anwendungsprogramme, reproduziert sich selbst und verbreitet sich so als bösartiger Bestandteil von Dateien und/oder Anwendungsprogrammen auf andere Computersysteme. Deshalb ist es nicht verwunderlich, dass für diese schädliche Software der Begriff "Virus" geprägt wurde, da sie ein ähnliches Verhalten wie biologische Viren aufweist.

Am gefährlichsten sind Viren, die das Betriebssystem attackieren. Ein solches Virus kann beispielsweise zur Folge haben, dass Sie Ihr gesamtes Betriebssystem installieren oder sogar Ihre Festplatte neu formatieren müssen. Ferner müssen Sie sicherstellen, dass alle Ihre gesicherten Dateien nicht von Viren infiziert wurden.

Einige dieser Viren wie z.B. CDEF und WDEF infizieren lediglich die Schreibtischdateien Ihres Macintosh (dies ist nur bis zum Betriebssystem Mac

OS 9 möglich). Bei den Schreibtischdateien handelt es sich um zwei Dateien, in denen Informationen über die Zuordnung von Symbolen zu Dateien und Anwendungsprogrammen gespeichert sind. Diese Viren infizieren keine anderen Dateien, verbreiten sich aber sehr schnell, da beim Anmelden eines Datenträgers als erstes die Schreibtischdateien gelesen werden.

Andere Systemviren wie beispielsweise die verschiedenen Versionen des Virus SevenDust können die Systemdatei, Kontrollfelder und Anwendungsprogramme infizieren. An einem bestimmten Datum und zu einer bestimmten Uhrzeit werden alle Dateien, bei denen es sich nicht um Anwendungsprogramme handelt, vom Systemdatenträger gelöscht.

Einige Viren agieren sehr schnell, während andere ihr übles Werk erst nach einer bestimmten Zeit verrichten. Einige Viren verbreiten sich lediglich auf andere Datenträger. Jedes Systemvirus kann prinzipiell Schäden verursachen.

## Trojanische Pferde

Die Bezeichnung "Trojanisches Pferd" stammt aus dem Trojanischen Krieg, in dem die alten Griechen laut ihrer Mythologie die Stadt Troja belagerten. Es handelte sich dabei um ein riesiges, innen hohles Pferd aus Holz, das die Griechen bauten und den Trojanern als eine Art Geschenk überließen, bevor sie sich an der Küste Trojas einschifften, um angeblich nach Hause zu segeln. Obwohl einige Trojaner dieses Geschenk mit großer Skepsis betrachteten, wurde es in die Stadt Troja gezogen. In der darauffolgenden Nacht sprangen mehrere im Innern des Trojanischen Pferds verborgene griechische Krieger

heraus und öffneten heimlich die Tore der Stadt, sodass Troja von den nun erneut heranstürmenden Griechen erobert werden konnte.
Es ist offensichtlich, dass den Trojanern niemals erzählt wurde, sie sollten keine unerbetenen Geschenke annehmen. Die Trojanischen Pferde unserer Zeit sind Computerprogramme, die zunächst harmlos wirken und angeblich eine bestimmte Aufgabe erfüllen. In Wirklichkeit enthalten diese Programme aber schädlichen Programmcode oder ein Virus. In vielen Fällen sind Trojanische Pferde gefährlicher als Viren. Einige Beispiele hierfür sind das Trojanische Pferd ChinaTalk, das sich als Systemerweiterung tarnt, aber Ordner löscht, und das bekannte Trojanische Pferd MacMag, das Systemdateien infiziert.

## Würmer

Würmer gehören zu den ältesten bösartigen Computerprogrammen. Sie verbreiten sich nicht, indem sie sich selbst in Dateien und Anwendungsprogramme einbetten, und sind nicht leicht zu finden. Der zuletzt aufgetauchte Macintosh-Wurm mit der Bezeichnung AutoStart erzeugt unsichtbare Dateien, die Daten und Dateien zerstören können.

Würmer verwenden zu ihrer Verbreitung Systemfunktionen. Der Wurm AutoStart verbreitet sich beispielsweise von infizierten CD-ROMs, indem er die Funktion des Macintosh-Betriebssystems zum automatischen Starten des Abspielens einer CD-ROM ausnutzt. Hierbei werden unsichtbare Systemerweiterungen erzeugt, die bei jedem Systemstart aktiviert werden.

## Dateiviren

Dateiviren unterscheiden sich insofern von Systemviren, als sie sich selbst in Datendateien und nicht in Programmdateien einbetten. Sie wirken nur dann schädlich, wenn auf dem betreffenden Macintosh ein bestimmtes Anwendungsprogramm installiert ist. Vor Kurzem aufgetauchte Viren, die ausschließlich Windows-Computer attackieren, sind die besonders schädlichen Viren Melissa und LoveBug. Diese Viren wurden durch e-Mail-Anhänge verbreitet, die nach dem Öffnen bestimmte Funktionen von Windows-Anwendungsprogrammen aktivierten. Man könnte nun denken, dass es sich hierbei um Trojanische Pferde handelt, doch ist ein Trojanisches Pferd ein Anwendungsprogramm, das vortäuscht, eine bestimmte Aufgabe zu erfüllen, während die beiden vorgenannten Dateiviren nichts anderes als in Dateien eingebetteter Programmcode sind.

## Makroviren

Dateiviren sind im Allgemeinen Makroviren. Diese Virenkategorie ist heutzutage die gefährlichste für Macintosh-Benutzer.

Das erste echte Makrovirus hieß "Concept"; es attackierte Microsoft-Word-Dateien. Varianten dieses Makrovirus folgten Schlag auf Schlag, da die Virenprogrammierer aufgrund der Verwendung des Textverarbeitungsprogramms Microsoft Word durch Millionen von Computerbenutzern die Möglichkeit sahen, wirklich großen Schaden anzurichten. Später wurden auch Makroviren speziell für Microsoft Excel

programmiert. Seitdem das erste Makrovirus vor ca. 5 Jahren auftauchte, wurden Tausende von Makroviren programmiert.

Die große, von Makroviren ausgehende Gefahr besteht darin, dass es sich um die ersten Viren für unterschiedliche Computerplattformen handelt. Über viele Jahre konnten sich die Benutzer von Macintosh-Computern relativ gut vor Viren geschützt fühlen, da es für den Macintosh nur ein paar Dutzend Viren gab, während sich die Windows-Benutzer mit Tausenden von Viren herumschlagen mussten. Doch nun, seit dem Auftauchen der ersten Makroviren, sehen sich auch Macintosh-Benutzer mit einem wirklichen Virenproblem konfrontiert.

Viele Anwendungsprogramme sind in der Lage, Makrobefehle zu generieren. Makroprogramme verwenden entweder interne Funktionen des Anwendungsprogramms wie z.B. von AppleWorks, um häufig verwendete Befehlsfolgen "aufzunehmen" und wieder "abzuspielen". Andere Programme wie Nisus Writer stellen eine leistungsfähigere Makrobefehlssprache zur Verfügung, die sowohl Menübefehle als auch eine Programmiersprache beinhaltet. Die Makrobefehlsfunktionen von Anwendungsprogrammen wie Microsoft Word und Microsoft Excel basieren auf Visual Basic, einer Programmiersprache, die große Ähnlichkeiten mit der Programmiersprache BASIC aufweist.
Einer der Gründe, weshalb sich Virenprogrammierer auf Makroviren für Anwendungsprogramme von Microsoft spezialisiert haben, ist, dass diese Programme Makrobefehle in Datendateien einbetten können. In der Vergangenheit musste man lediglich befürchten, dass ein Computer über Anwendungsprogramme aus obskuren Quellen mit Viren infiziert wird. Der

Grund hierfür war, dass ein Virus selbst ein Programm ist, das nur in Aktion treten kann, wenn das Wirtsprogramm (das Anwendungsprogramm, in dem das Virus eingebettet ist) gestartet wird. Bei Microsoft Visual Basic ist das anders: Ein Makrobefehl kann von einer Vorlage gestartet oder in eine Datendatei eingebettet werden. Die Benutzer waren nach dem Auftauchen der ersten Makroviren recht verwundert, da sie annahmen, dass beim Öffnen einer Word- oder Excel-Datei keine Befehle ausgeführt werden. Doch diese Dateien können Makrobefehle enthalten, die vollkommen unerwartete Aktionen ausführen.

Wenn die Makrobefehlssprache die Möglichkeit bietet, Dateien zu verändern, kann sich ein Makrovirus in andere Dateien kopieren, die vom gleichen Anwendungsprogramm (also z.B. Word oder Excel) verwendet werden. Dies ermöglicht es dem Virus, sich zu verbreiten, indem Dateien geöffnet, neue Dateien erstellt oder Dateien an andere Personen weitergegeben werden.

Die meisten Makroviren für Microsoft Word verwenden Befehle wie AutoOpen, AutoClose, AutoExec und AutoExit. Hierbei handelt es sich um Befehle, die ausgeführt werden, wenn eine bestimmte Aktion stattfindet. Diese vier Aktionen werden beim Arbeiten mit jeder Datei ausgeführt. Wenn ein Makrovirus beispielsweise so programmiert wäre, dass es sich nur dann in eine andere Datei kopiert, wenn ein bestimmter Menübefehl aufgerufen wird, würde es sich mit geringerer Geschwindigkeit verbreiten.

Deshalb treten die meisten Makroviren bereits beim Öffnen einer Datei in Aktion, um sich dann in die gleichzeitig geöffnete Vorlage zu kopieren. Diese Vorlage wird nicht eigens vom Benutzer, sondern automatisch im Hintergrund

geöffnet. Vorlagen enthalten bestimmte Anpassungsinformationen und auch zulässige Makrobefehle, die vom Benutzer in der Vorlage gespeichert wurden.

Das häufigste Makrovirus für Microsoft Word kopiert sich selbst in die momentan aktive Vorlage, ändert einige Menüoptionen, sodass die Vorlage nicht mehr geändert werden kann, ändert den Dateityp (wodurch die zugeordneten Symbole geändert werden, sodass die Dateien im Finder als Vorlagen erscheinen) und kopiert nun das Makrovirus aus der infizierten Vorlage in alle zukünftig geöffneten oder neu erstellten Dateien. Dieses Makrovirus kann gelöscht werden, indem die aktive Vorlagendatei und alle infizierten Dateien gelöscht werden.

Andere Makroviren können noch weitaus gefährlicher werden. Sie können Ihre Dateien beschädigen oder löschen, bestimmte Funktionen des entsprechenden Anwendungsprogramms unzugänglich machen, und vieles mehr. Makroviren sind plattformunabhängig, d.h. sie sind sowohl für PCs mit dem Betriebssystem Windows als auch für Macintosh-Computer gefährlich.

Makrobefehlssprachen sind sehr nützliche Hilfsmittel, die einem Computerbenutzer seine Arbeit ungemein erleichtern können. Nicht alle Makrobefehle sind Makroviren. Microsoft Word verfügt über die Möglichkeit, festzulegen, dass in einer Word-Datei enthaltene Makrobefehle nicht ausgeführt werden. Hierdurch verzichtet der Computerbenutzer jedoch auf die unter Umständen sehr nützlichen Makrobefehlsfunktionen. Ein großes Problem besteht darin, dass Makrobefehle meistens in Datendateien und nicht in separaten Makrobefehlsdateien gespeichert werden. (Bei manchen Anwendungsprogrammen wie z.B. Nisus Writer ist dies jedoch der Fall.) Wenn

Makrobefehle nur in speziellen Makrobefehlsdateien gespeichert wären, könnten Makrobefehle problemlos von Computerbenutzern untereinander ausgetauscht werden. Gleichzeitig wäre sichergestellt, dass geöffnete Dokumentendateien lediglich Daten enthalten. Unglücklicherweise führt das Einbetten von Makrobefehlen in Datendateien dazu, dass viele Computerbenutzer Angst vor Makrobefehlen haben und sie nicht für den Zweck nutzen wollen, für den sie ursprünglich vorgesehen wurden: nämlich um ihnen ihre Arbeit zu erleichtern.

Intego VirusBarrier X erkennt alle bekannten Word- und Excel-Makroviren und wird aktualisiert, wenn neue Makroviren auftauchen.

## Falsche Viruswarnungen

In den letzten Jahren mehrten sich die Fälle, in denen der eine oder andere "Spaßvogel" e-Mail-Mitteilungen versandte oder Warnungen in Foren veröffentlichte, mit denen er vor Viren warnte, die es überhaupt nicht gab. Diese falschen Viruswarnungen führen dazu, dass Computerbenutzer in Panik geraten und alle ihre Bekannten über diese vermeintliche Virusgefahr informieren, sodass innerhalb kürzester Zeit eine weltweite Panik entsteht.

Einer der angeblichen, aber nicht existenten Viren, vor dem weltweit die meisten Warnungen verbreitet wurden, war Good Times. Diese Bezeichnung entspricht dem Betreff in der entsprechenden e-Mail-Mitteilung, die angeblich dieses Virus enthalten sollte. Obwohl sich schnell herausstellte, dass es dieses Virus gar nicht gab und vor ihm bereits im Jahre 1994 gewarnt wurde, kursieren die e-Mail-Mitteilungen mit einer Warnung vor diesem Virus auch heute immer noch im Internet. Immer wieder tauchen neue Warnungen vor angeblichen Viren auf; die Tendenz ist steigend.

Diese falschen Viruswarnungen können sich nur so stark verbreiten, weil die meisten Internet-Benutzer zu wenig von Computerviren wissen. Die meisten dieser Falschmeldungen erwecken den Eindruck, es handle sich um eine tatsächliche Virusgefahr, und gelegentlich scheinen diese Viruswarnungen sogar von einem seriösen Unternehmen der Computerbranche zu stammen. Trotzdem handelt es sich aber auch bei derartigen Viruswarnungen um nichts anderes als üble Scherze.

Wenn Sie Mitarbeiter in einem Unternehmen sind und eine solche Viruswarnung erhalten, sich aber nicht sicher sind, ob es sich nicht doch um eine echte Viruswarnung handelt, sollten Sie sich sofort an den Netzwerk- oder Systemverwalter Ihres Unternehmens wenden, um herauszufinden, ob die Virusgefahr real ist. Wenn Sie Ihren Macintosh nur privat einsetzen, können Sie sich auf der Intego-Website www.intego.com informieren. Intego informiert seine Kunden und Interessenten stets sofort über jede neu auftauchende Virusgefahr. Das Virus Monitoring Center von Intego ist rund um die Uhr und an allen Tagen des Jahres besetzt, und reagiert sofort auf das Auftauchen jedes neuen Virus.

Wenn Sie befürchten, dass Ihr Macintosh von einem neuen Virus infiziert wurde, gehen Sie bitte gemäß den entsprechenden Hinweisen im Kapitel 7 (Diagnose) dieses Benutzerhandbuchs vor. Dort ist beschrieben, wie Sie Ihren Macintosh auf Virenbefall diagnostizieren und wie Sie das Virus Monitoring Center von Intego kontaktieren können.

## Wie verbreiten sich Computerviren?

Computerviren können sich auf unterschiedliche Art und Weise verbreiten. Prinzipiell bestehen hier zwei Möglichkeiten: über Dateien oder auswechselbare Datenträger. Datenträger wie CD-ROMs, Zip-Disketten usw. für den Macintosh enthalten unsichtbare Dateien, die als Schreibtischdateien bezeichnet werden. Diese Dateien enthalten vom Betriebssystem genutzte Informationen wie Dateisymbole und Anwendungsprogramme. Viren, von denen die Schreibtischdateien infiziert werden, können sich verbreiten, wenn

Sie einen auswechselbaren Datenträger ins entsprechende Laufwerk einlegen, da jeder Macintosh beim Anmelden eines Datenträgers zuerst die Schreibtischdateien ausliest. Intego VirusBarrier X schützt Ihren Macintosh vor diesen Viren, indem die Schreibtischdateien auf jedem Datenträger nach Viren durchsucht werden, bevor sich diese ausbreiten können. Wenn Intego VirusBarrier X in den Schreibtischdateien ein Virus findet, wird dieses aus den Schreibtischdateien gelöscht, noch bevor diese vom Betriebssystem gelesen werden.

Viren können auch über infizierte Dateien verbreitet werden. Diese Dateien können auf CD-ROMs oder anderen auswechselbaren Datenträgern enthalten sein oder übers Internet heruntergeladen werden. Viren können auch als Anhänge von e-Mail-Mitteilungen versandt werden. Mit Viren infizierte Dateien können die Viren erst verbreiten, nachdem die Dateien geöffnet worden sind. Durch das bloße Kopieren eines Anwendungsprogramms kann ein Virus nicht verbreitet werden. Dies ist nur dann möglich, wenn das Wirtsprogramm gestartet wird. Das Gleiche gilt für Datendateien: wenn Sie eine Datei erhalten, die ein Makrovirus enthält, kann nichts geschehen, bevor Sie diese Datei geöffnet haben. Intego VirusBarrier X schützt Ihren Macintosh vor diesen Viren, indem die Dateien auf Ihren Datenträgern beim Öffnen oder Schreiben nach Viren durchsucht werden. In dem Moment, in dem Sie eine Datei öffnen, wird sie von Intego VirusBarrier X nach Viren durchsucht. Wenn Intego VirusBarrier X ein Virus erkennt, wird die betreffende Datei oder das betreffende Anwendungsprogramm repariert oder im schlechtesten Fall unbrauchbar gemacht.

## Wie können Sie Ihren Macintosh vor Viren schützen?

Durch einige einfache Vorsichtsmaßnahmen können Sie sicherstellen, dass Ihr Macintosh nicht von Computerviren befallen wird. Zunächst einmal sollten Sie Intego VirusBarrier X installieren, sodass diese Antivirussoftware Ihren Macintosh kontinuierlich und automatisch auf Viren überwacht. Intego VirusBarrier X ist der optimale Schutz für Ihren Macintosh. Dieses Antivirusprogramm arbeitet im Hintergrund und stellt jederzeit sicher, dass Ihr Macintosh nicht von Viren befallen wird.

Um zu gewährleisten, dass Intego VirusBarrier X auch die allerneuesten Viren erkennen kann, muss die Antivirussoftware regelmäßig aktualisiert werden. Dies kann die in Intego VirusBarrier X integrierte Funktion NetUpdate übernehmen; auch eine automatische Aktualisierung ist möglich. Sie sollten die Prüfung nach einer neue Version von Intego VirusBarrier X mindestens einmal im Monat durchführen lassen. Am besten besuchen Sie regelmäßig die Intego-Website www.intego.com, um festzustellen, ob neue Macintosh-Viren aufgetaucht sind, sodass Intego VirusBarrier X aktualisiert werden muss.

Ebenfalls von großer Wichtigkeit ist, dass Sie auf Ihrem Macintosh ausschließlich Software verwenden, die Sie aus einer zuverlässigen Quelle erhalten haben. In vielen Fällen enthält illegale Software Viren oder Trojanische Pferde. Installieren Sie grundsätzlich nur Software, bei der Sie wissen, dass es sich um Originalsoftware vom jeweiligen Softwarehersteller handelt. Intego VirusBarrier X schützt Ihren Macintosh, indem bei jeder Softwareinstallation alle zu installierenden Dateien auf Viren geprüft werden.

Ferner sollten Sie sich vor e-Mail-Anhängen und anderen übers Internet versandten Dateien hüten. Sie wissen, dass der älteste bisher bekannte Fall, in dem ein unerwartetes, zweifelhaftes "Geschenk" angenommen wurde, zur Zerstörung einer ganzen Stadt geführt hat, nämlich als die Trojaner das ihnen am Strand von Troja hinterlassene Geschenk der Griechen in ihre Stadt gezogen hatten. Vielleicht wurden auch Sie bereits gewarnt, niemals einen e-Mail-Anhang zu öffnen, den Ihnen ein Unbekannter geschickt hat. Doch in letzter Zeit haben sich Windows-Viren mit rasender Geschwindigkeit verbreitet, die nicht von Fremden, sondern von Bekannten und Kollegen an PC-Benutzer versandt wurden. Auf alle Fälle sollten Sie einen e-Mail-Anhang, den Sie von einer Ihnen unbekannten Person erhalten haben, niemals öffnen. Dadurch ist allerdings nicht sichergestellt, dass Sie nicht auch einmal ein Virus von einem Freund oder Kollegen erhalten, das dieser unwissentlich verbreitet. Intego VirusBarrier X schützt Ihren Macintosh, indem jede von Ihnen geöffnete Datei auf Viren durchsucht wird. Gefundene Viren werden automatisch eliminiert. Wenn Ihr Macintosh mit einem Netzwerk verbunden ist und Intego VirusBarrier X in einem e-Mail-Anhang ein Virus erkennt, sollten Sie sich sofort an Ihren Netzwerkverwalter wenden, sodass dieser die infizierte Datei vom e-Mail-Server Ihres Unternehmens entfernen kann.

Trotz des von Intego VirusBarrier X gebotenen Schutzes vor Viren sollten Sie eines tun, um Ihre Daten zu schützen: regelmäßig eine Datensicherung Ihrer Dateien anlegen. Wichtige Dateien sollten mindestens einmal pro Tag gesichert werden. Am besten ist es, von allen Dateien mehrere Datensicherungen zu erstellen. Der Grund für die Notwendigkeit mehrerer Datensicherungen besteht darin, dass die Datenträger, auf denen die gesicherten Daten gespeichert sind, beschädigt werden oder verloren gehen können, sodass Sie in diesen Fällen

über keine Datensicherung verfügen. Die Software Intego Personal Backup X stellt eine umfassende Datensicherungslösung dar. Dieses Programm kann Ihre Dateien automatisch sichern, sodass Sie jederzeit über Kopien Ihrer Dateien verfügen. Insofern bietet Intego Personal Backup X zusätzlichen Schutz vor Viren.

Eine gute Datensicherungsstrategie wäre die folgende: Nehmen wir einmal an, dass Sie Ihre Dateien auf einer Zip-Diskette sichern. In diesem Fall sollten Sie mindestens zwei verschiedene Zip-Diskette verwenden, wobei Sie Ihre Daten beispielsweise am Montag auf der Zip-Diskette Nr. 1, am Dienstag auf der Zip-Diskette Nr. 2, am Mittwoch wieder auf der Zip-Diskette Nr. 1 usw. sichern. Durch die Anwendung dieser Datensicherungsstrategie ist Ihr Macintosh sehr gut abgesichert. Wenn Dateien auf der internen Festplatte Ihres Macintosh mit Viren infiziert sind, verfügen Sie immer noch über Kopien dieser Dateien auf einer der beiden Zip-Disketten. Dadurch, dass Sie Ihre Dateien gesichert haben, können Sie auch ansonsten katastrophale Probleme wie beispielsweise einen Totalausfall Ihres internen Festplattenlaufwerks lösen. Dank der relativ geringen Kosten auswechselbarer Datenträger, einmal oder mehrmals beschreibbarer CD-Rs, externer Festplattenlaufwerke usw. dürfte es keinen Grund geben, nicht auch das komplette Macintosh-Betriebssystem sowie alle Anwendungsprogramme zu sichern, obwohl dies nicht sehr häufig getan werden muss. Denken Sie daran, dass die Dateien auf Ihren Macintosh durch Viren oder auf andere Weise unbrauchbar werden können! Die Neuinstallation Ihres Betriebssystems und Ihrer Anwendungsprogramme kann viele Stunden lang dauern. Wenn Sie aber sämtliche Dateien auf der internen Festplatte Ihres Macintosh gesichert haben, können Sie diese Dateien innerhalb weniger Minuten wiederherstellen.

# 3 - Installation

## Systemanforderungen

- Jeder für Mac OS X geeignete Macintosh
- Mac OS X 10.1.1 oder neuer, Mac OS X Server 10.1.1 oder neuer
- Freie Festplattenspeicherkapazität von mindestens 20 MByte
- Bildschirmdarstellung von minimal 800 x 600 Bildpunkten

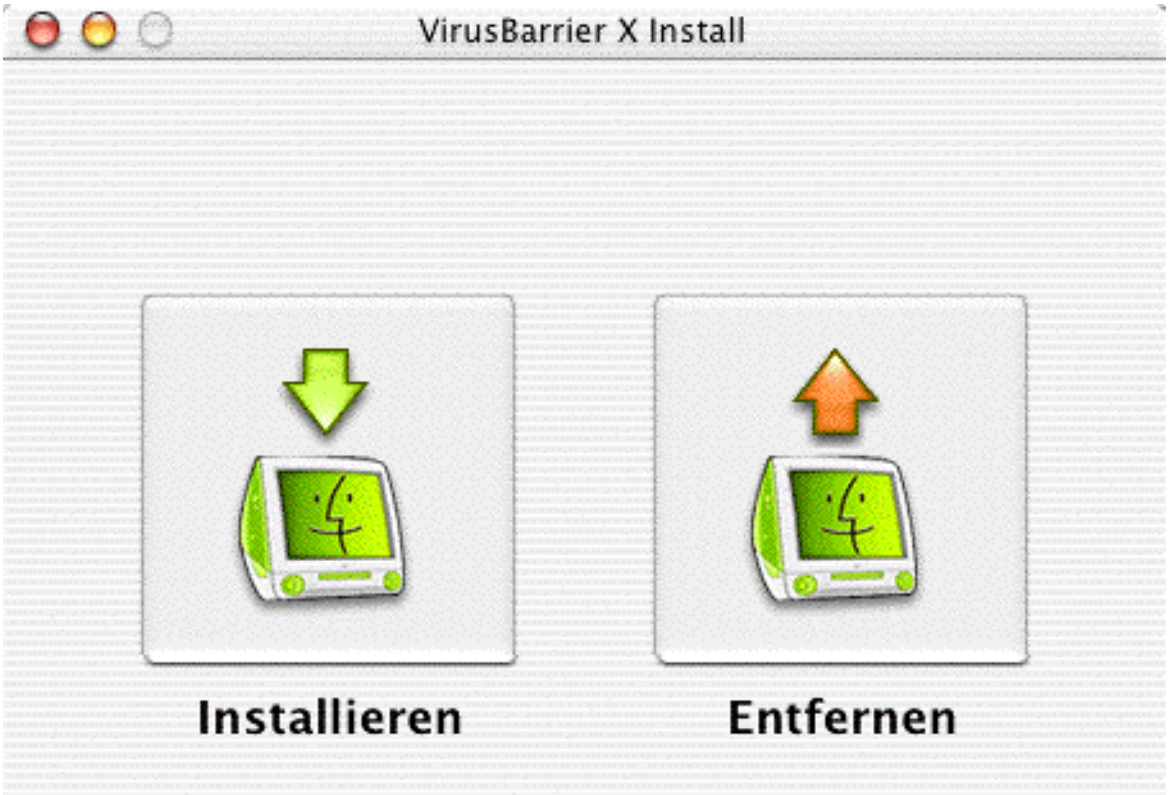
## Installieren von Intego VirusBarrier X

Die Installation von Intego VirusBarrier X ist sehr einfach. Legen Sie die CD-ROM mit Intego VirusBarrier X ins CD-ROM-Laufwerk Ihres Macintosh ein. Nun wird ein Fenster geöffnet, in dem Sie das Installationsprogramm für Intego VirusBarrier X, eine Datei namens "Bitte lesen", das Benutzerhandbuch zu Intego VirusBarrier X (die .pdf-Datei, die Sie gerade lesen) und ein Programm zum Installieren des Acrobat Reader (eines Programms zum Lesen von .pdf-Dateien) sehen. (Wenn Sie Intego VirusBarrier X direkt auf der Intego-Website gekauft und von dort heruntergeladen haben, finden Sie in demjenigen Ordner, in den Sie normalerweise Dateien aus dem Internet herunterladen, eine Datei namens "Intego VirusBarrier X Install.dmg". Doppelklicken Sie aufs Symbol dieser Datei. Das Symbol des Datenträgerabbilds erscheint nun wie das Symbol einer gewöhnlichen Festplatte auf dem Schreibtisch Ihres Macintosh.)

Lesen Sie bitte die Datei "Bitte lesen". Diese enthält die neuesten Informationen über Intego VirusBarrier X.

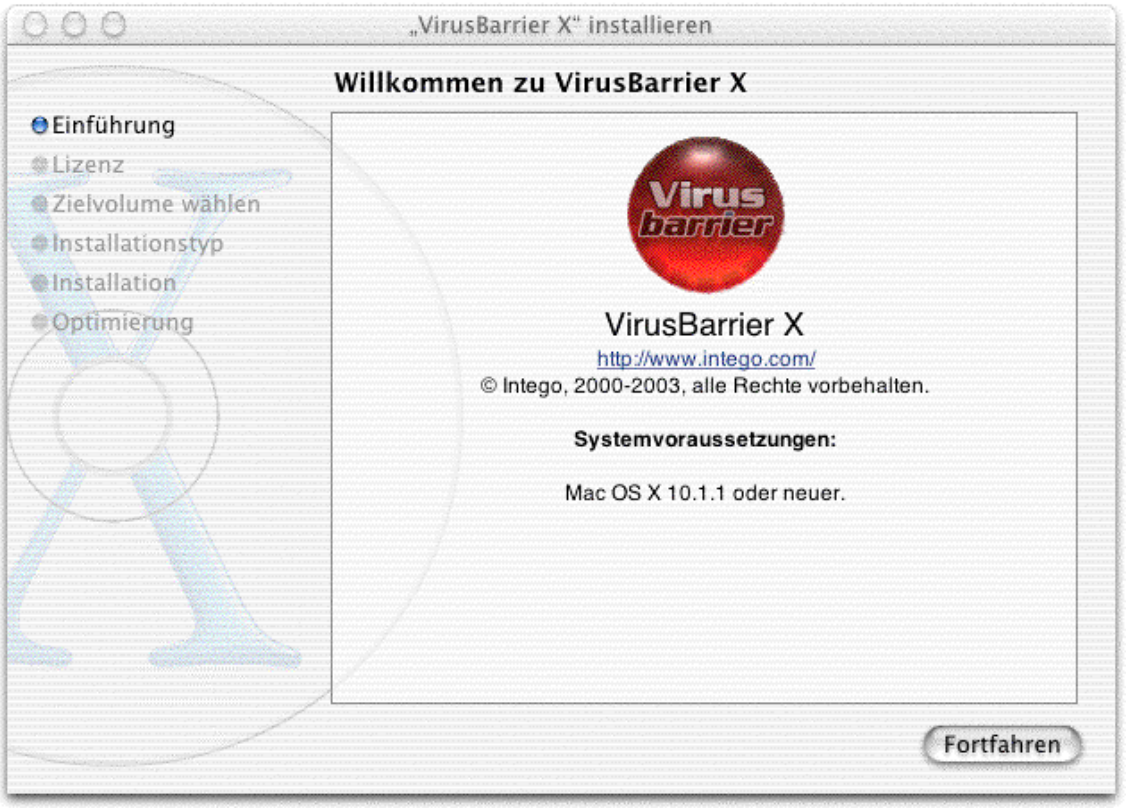
Doppelklicken Sie nun aufs Symbol des Programms "Intego VirusBarrier X Install".

Das Installationsprogramm bietet Ihnen zwei Optionen zur Auswahl an: "Installieren" und "Entfernen".




Wenn Sie Intego VirusBarrier X installieren wollen, müssen Sie auf die Schaltfläche "Installieren" klicken. Wenn Sie Intego VirusBarrier X entfernen wollen, müssen Sie auf die Schaltfläche "Entfernen" klicken.

Nun wird ein Fenster geöffnet, in das Sie ein Administratorpasswort eingeben müssen, um Intego VirusBarrier X installieren zu können. Klicken Sie aufs Schlosssymbol und geben Sie Ihr Administratorpasswort ein. Wenn Sie OS X 10.2 oder neuer verwenden, müssen Sie Ihr Administratorpasswort ins geöffnete Fenster eingeben. Geben Sie Ihr Administratorpasswort ein und klicken Sie dann auf die Schaltfläche "OK". Nun wird das nachstehend gezeigte Fenster geöffnet:

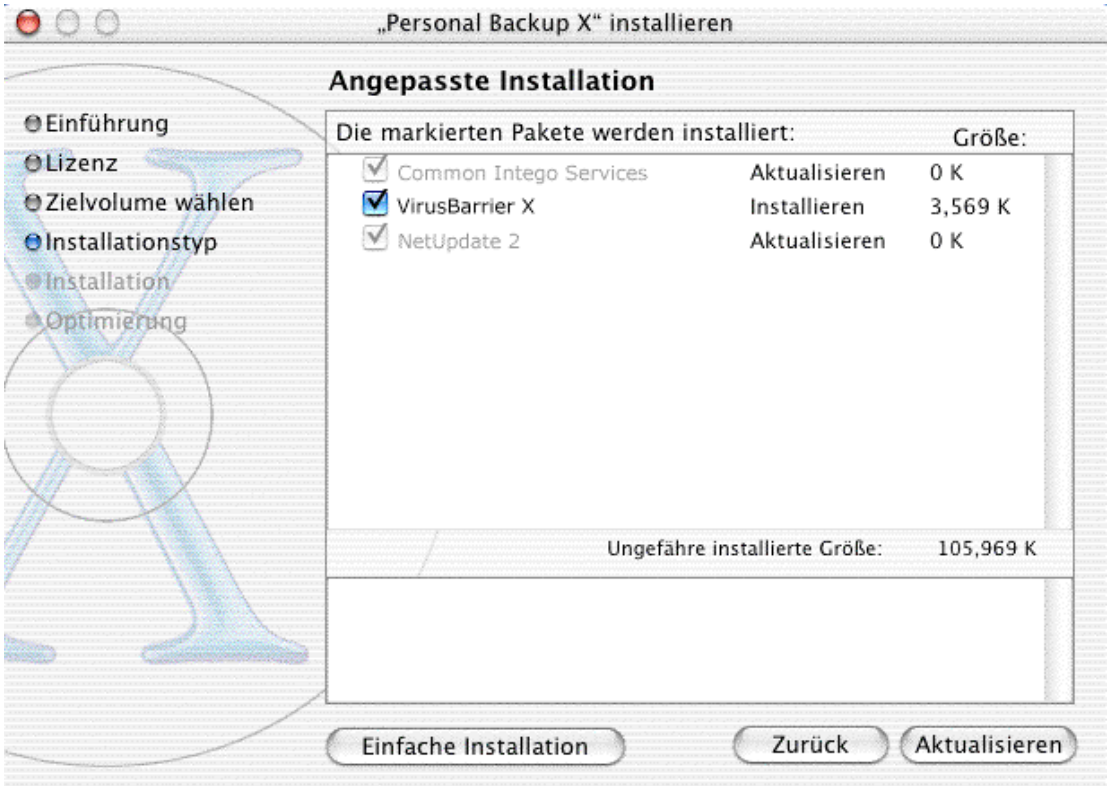



Klicken Sie auf die Schaltfläche "Fortfahren", um die Installation fortzusetzen. Hierauf wird die Intego-Softwarelizenzvereinbarung angezeigt. Klicken Sie zuerst auf die Schaltfläche "Fortfahren" und dann auf die Schaltfläche "Annehmen", um die Bedingungen der Intego-Softwarelizenzvereinbarung zu

akzeptieren. Wenn Sie die Intego-Softwarelizenzvereinbarung nicht akzeptieren wollen, müssen Sie auf die Schaltfläche "Ablehnen" klicken, worauf das Installationsprogramm automatisch beendet wird.

Im nächsten Fenster sehen Sie die Symbole aller für Ihren Macintosh verfügbaren Datenträger. Wählen Sie den Datenträger, auf dem Intego VirusBarrier X installiert werden soll, und klicken Sie dann auf die Schaltfläche "Fortfahren".

Klicken Sie auf die Schaltfläche "Installieren", um eine Standardinstallation von Intego VirusBarrier X durchzuführen. Wenn Sie eine benutzerspezifische Installation durchführen wollen, müssen Sie auf die Schaltfläche "Anpassen" klicken. Nun wird das nachstehend gezeigte Fenster geöffnet:



In diesem Fenster können Sie die zu installierenden Softwarekomponenten wählen. Wie Sie sehen können, wird das Kästchen links von "Common Intego Services" grau dargestellt, sodass Sie diese Softwarekomponente nicht abwählen können. Sie können Intego VirusBarrier X und/oder NetUpdate installieren. Wenn auf Ihrem Macintosh bereits andere Intego-Programme installiert sind, ist die Schaltfläche "Aktualisieren" nicht grau dargestellt. Dies bedeutet, dass bestimmte Softwarekomponenten, die gemeinsam von allen Intego-Anwendungsprogrammen verwendet werden, nicht erneut installiert werden.

Nach der Installation werden Sie aufgefordert, Ihren Macintosh neu zu starten.

## Registrieren von Intego VirusBarrier X

Öffnen Sie nach dem Neustart Ihres Macintosh das Programm Intego VirusBarrier X, das sich im Ordner "Programme" befindet. Intego VirusBarrier X startet nun sein internes Registrierungsprogramm. Hierauf wird das nachstehend gezeigte Fenster geöffnet:

Da Mac OS X ein Mehrbenutzer-Betriebssystem ist, haben nicht alle Benutzer eines Macintosh die gleichen Privilegien. Nach dem erstmaligen Starten von Intego VirusBarrier X kann zwar jeder Benutzer die Seriennummer der Software eingeben, aber nur ein Benutzer mit Administratorprivilegien kann Intego VirusBarrier X konfigurieren.

Geben Sie in dieses Fenster bitte Ihren Namen, den Namen Ihres Unternehmens (sofern zutreffend) und Ihre Seriennummer ein. Die Seriennummer finden Sie

auf dem Aufkleber auf der CD-ROM mit Intego VirusBarrier X. Nach der Registrierung wird Intego VirusBarrier X automatisch gestartet. Wenn Sie der Administrator Ihres Macintosh sind, können Sie die Software konfigurieren.

## Verwenden von Intego VirusBarrier X im Demonstrationsmodus

Intego VirusBarrier X kann maximal 30 Tage lang im Demonstrationsmodus laufen, um Ihnen die Leistungsfähigkeit dieses Antivirusprogramms zu verdeutlichen, bevor Sie es kaufen. Wenn Sie den Demonstrationsmodus von Intego VirusBarrier X aktivieren wollen, müssen Sie im Fenster "Serialisierung" auf die Schaltfläche "Demo" klicken. Nun wird ein Fenster geöffnet, in dem Sie gefragt werden, ob Sie Intego VirusBarrier X im Testmodus laufen lassen wollen. Falls ja, müssen Sie auf die Schaltfläche "Testmodus" klicken. Falls nein, klicken Sie bitte auf die Schaltfläche "Abbrechen".

# 4 - Erste Schritte

## Der Standardmodus von Intego VirusBarrier X

Wenn Sie Ihren Macintosh nach der Installation von Intego VirusBarrier X neu starten, beginnt die Antivirussoftware automatisch damit, Ihren Macintosh kontinuierlich auf verdächtige Aktivitäten zu überwachen. Intego VirusBarrier X ist ein besonders einfach zu bedienendes und absolut unaufdringliches Antivirusprogramm. Es schützt Ihren Macintosh, ohne dass Sie selbst etwas dazu tun müssen.

Nach der Installation können Sie Intego VirusBarrier X einfach im Hintergrund laufen lassen. Allerdings sollten Sie sicherstellen, dass NetUpdate automatisch auf neue Versionen von Intego VirusBarrier X auf dem Intego-Server prüft. Alternativ können Sie diese Funktion auch manuell starten. In diesem Fall sollten Sie das mindestens einmal pro Monat tun.

Doppelklicken Sie aufs Symbol von Intego VirusBarrier X im Ordner "Programme", um das Antivirusprogramm zu starten. Nun können Sie die Einstellungen des Antivirusprogramms ändern oder eine manuelle Virensuche starten.

## Bedienungsoberfläche von Intego VirusBarrier X

Die Bedienungsoberfläche von Intego VirusBarrier X sieht wie folgt aus. Oben befindet sich eine Art Kugel für die funktionsabhängige Bedienung. Darunter finden Sie mehrere Schaltflächen für die Auswahl von Einstellungen und das

Starten der Virensuche. Wenn Sie auf eine dieser Schaltflächen klicken, wird ein Schieber geöffnet.

**Die Kugel von Intego VirusBarrier X**
In dieser Kugel werden Informationen über die derzeit ausgeführten Aktionen angezeigt.

**Die kontextabhängige Schaltfläche**
Die Beschriftung dieser Schaltfläche ändert sich in Abhängigkeit von ihrer jeweiligen Funktion (Virensuche, Pause, Stopp usw.).

**Die Schaltfläche "Virensucher"**
Durch Klicken auf diese Schaltfläche können Sie wählen, welcher Datenträger, Ordner oder welche Datei nach Viren durchsucht werden soll

**Die Schaltfläche "Protokollieren"**
Beim Klicken auf diese Schaltfläche wird eine Protokollliste geöffnet. Hier wird angezeigt, wann (Tag / Uhrzeit) eine manuell gestartete Virensuche durchgeführt wurde, und welche infizierten oder beschädigten Dateien gefunden wurden.

**Die Schaltfläche "NetUpdate"**
Beim Klicken auf diese Schaltfläche wird die Suche nach der neuesten Version von Intego VirusBarrier X gestartet.

**Die Schaltfläche "Voreinstellungen"**
Nach dem Klicken auf diese Schaltfläche können Sie andere Einstellungen von Intego VirusBarrier X ändern.

**Die Schaltfläche "i"**
Wenn Sie auf diese Schaltfläche klicken, werden Informationen über Intego VirusBarrier X angezeigt.

Wenn Sie einen Schieber schließen wollen, müssen Sie nur nochmals auf die gleiche Schaltfläche oder aufs Dreieck rechts vom Schieber klicken. Sie können

auch auf eine andere Schaltfläche klicken, um den aktuell geöffneten Schieber zu schließen. Gleichzeitig wird der Schieber geöffnet, der zu der soeben von Ihnen geklickten Schaltfläche gehört.

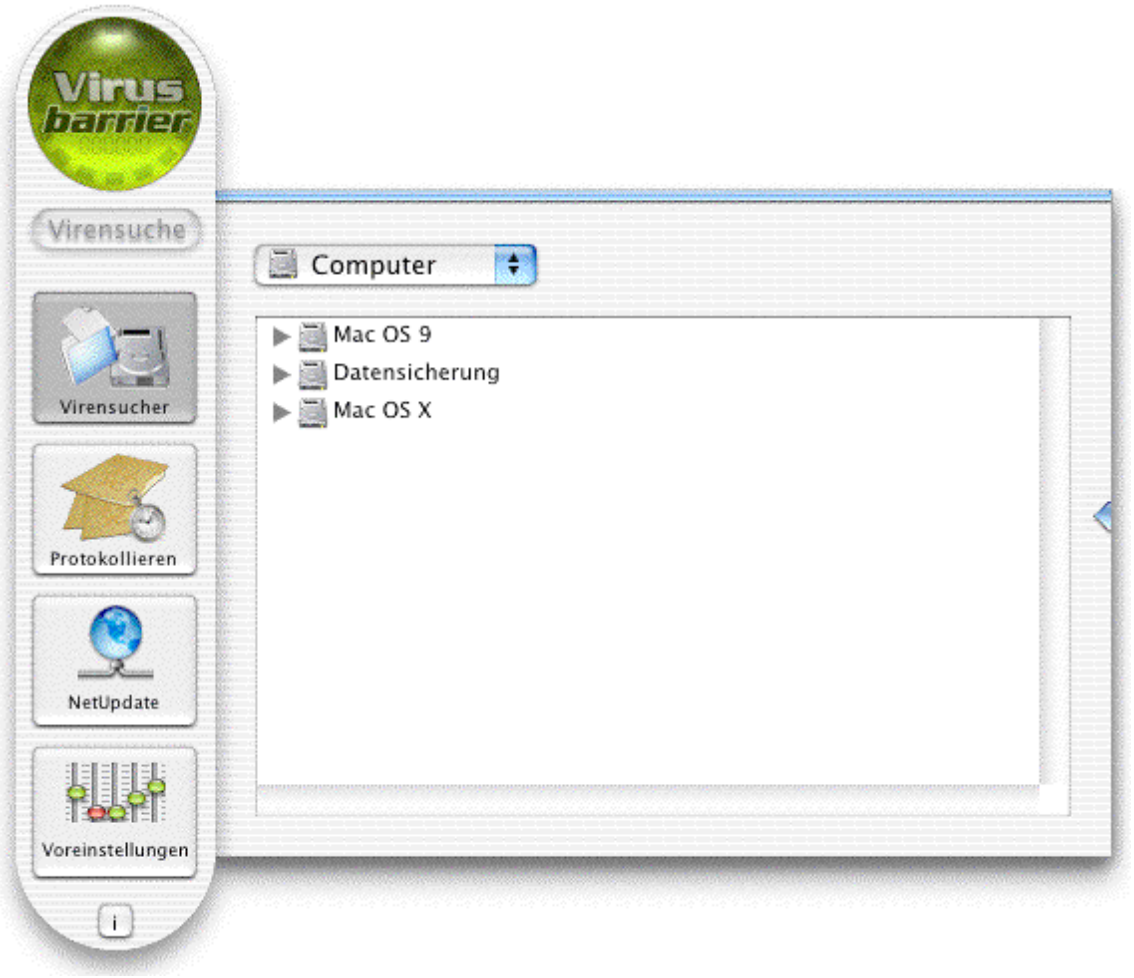
## Manuelles Starten einer Virensuche

Nach der Installation von Intego VirusBarrier X überwacht das Antivirusprogramm Ihren Macintosh, um sicherzustellen, dass er nicht mit einem Virus infiziert wird. Intego VirusBarrier X prüft jede Datei beim Lesen oder Schreiben. Unmittelbar nach der Installation von Intego VirusBarrier X können Sie alle Ihre Dateien auf Viren untersuchen lassen, um sicherzugehen, dass alle Dateien auf den bei Ihrem Macintosh angemeldeten Datenträgern virenfrei sind. Dies sollten Sie unbedingt tun, um eventuell vorhandene Viren zu eliminieren. Anschließend sorgt Intego VirusBarrier X automatisch dafür, dass Ihr Macintosh stets virenfrei bleibt.

Wenn Sie nach der Installation von Intego VirusBarrier X keine Virensuche gestartet haben und dies nachholen wollen, müssen Sie das Programm Intego VirusBarrier X starten, indem Sie auf sein Symbol im Ordner "Programme" doppelklicken.

Klicken Sie nun auf die Schaltfläche "Wählen". Hierauf wird ein Schieber mit einer Liste aller derzeit bei Ihrem Macintosh angemeldeten Datenträger geöffnet. In dieser Liste werden die Datenträger ähnlich wie im Finder dargestellt. Sie sehen hier Datenträger, Ordner und Dateien in hierarchischer Ordnung. Wenn Sie die Anzeige eines Datenträgers oder Ordners erweitern wollen, sodass Sie seinen Inhalt sehen können, müssen Sie nur aufs Dreieck

links vom entsprechenden Symbol klicken. Um die Anzeige eines Datenträgers oder Ordners zu minimieren, müssen Sie nur auf dieses Dreieck klicken.




Um einen Datenträger, einen Ordner oder eine Datei nach Viren zu durchsuchen, müssen Sie nur aufs entsprechende Symbol doppelklicken oder einmal darauf klicken und dann auf die Schaltfläche "Virensuche" klicken. In der Kugel für die funktionsabhängige Bedienung sehen Sie nun, dass die Virensuche gestartet wurde. In der Kugel wird die Anzahl der bereits durchsuchten Dateien angezeigt.

Wenn Sie in den Voreinstellungen die Option "Restliche Dateien anzeigen" gewählt haben, zeigt Intego VirusBarrier X die Anzahl und den Prozentsatz der noch zu durchsuchenden Dateien an. Wenn Sie auf die Kugel klicken, wird auf die Anzeige der bereits durchsuchten Dateien und des entsprechenden Prozentsatzes umgeschaltet.

Sie können die Virensuche jederzeit stoppen, indem Sie auf die Schaltfläche "Stopp" klicken. Wenn Sie die Virensuche vorübergehend anhalten wollen, müssen Sie die Umschalttaste in der Tastatureinheit Ihres Macintosh drücken. Hierauf ändert sich die Bezeichnung der Schaltfläche von "Stopp" in "Pause". Wenn Sie nun auf die Schaltfläche "Pause" klicken, wird die Virensuche vorübergehend angehalten.

Durch Klicken auf die gleiche Schaltfläche, die nun mit "Fortfahren" beschriftet ist, können Sie die Virensuche fortsetzen.

## Voreinstellungen von NetUpdate

Wenn Sie auf die Schaltfläche "NetUpdate" klicken, wird der Schieber "NetUpdate" geöffnet. Dieser Schieber ermöglicht es Ihnen, eine Prüfung auf eine neue Version von Intego VirusBarrier X durchführen zu lassen. Hier sehen Sie auch Informationen wie das Datum der letzten Prüfung auf eine neue Version, die Nummer der derzeit auf Ihrem Macintosh installierten Version von Intego VirusBarrier X, und das Ablaufdatum Ihres Abonnements auf Intego-Softwareaktualisierungen (sofern Ihr Abonnement gültig ist). Gleichzeitig mit dem Kauf von Intego VirusBarrier X erwerben Sie ein kostenloses Abonnement auf alle Aktualisierungen der Virendefinitionen über 1 Jahr.

Sie sollten Intego VirusBarrier X regelmäßig aktualisieren, um sicherzustellen, dass Ihr Macintosh auch vor den neuesten Viren geschützt ist. Im Lieferumfang von Intego VirusBarrier X ist das Programm NetUpdate von Intego enthalten, das automatisch prüfen kann, ob auf Ihrem Macintosh die jeweils neueste Version von Intego VirusBarrier X installiert ist. NetUpdate kann auch das Herunterladen der neuesten Version von Intego VirusBarrier X übernehmen.

Wenn Sie die Prüfung auf das Vorhandensein einer neuen Version von Intego VirusBarrier X auf dem Intego-Server manuell starten wollen, müssen Sie nur auf die Schaltfläche "Jetzt prüfen..." klicken. Hierauf wird Intego NetUpdate gestartet, stellt eine Verbindung mit dem Intego-Server her und prüft, ob dort

eine neue Version von Intego VirusBarrier X oder neue Virendefinitionen vorhanden sind. Gleichzeitig mit dem Kauf von Intego VirusBarrier X erwerben Sie ein kostenloses Abonnement auf alle Aktualisierungen der Virendefinitionen über 1 Jahr.

Sie können NetUpdate konfigurieren, indem Sie das Zeitintervall für automatische Prüfungen auf aktualisierte Software festlegen. Hierzu steht Ihnen "NetUpdate Preferences" in den "System Preferences" zur Verfügung.

Weitere Informationen über NetUpdate finden Sie im Abschnitt "Voreinstellungen von Intego VirusBarrier X" des Kapitels 6 und im NetUpdate-Benutzerhandbuch.

## Virensuche mit Ziehen und Ablegen

Sie können jeden Datenträger oder Ordner, und auch jede Datei auf Viren durchsuchen lassen, indem Sie sein / ihr Symbol einfach ins Fenster von Intego VirusBarrier X ziehen. Wenn Sie das jeweilige Symbol loslassen, wird das entsprechende Objekt auf die gleiche Weise wie beim manuellen Starten der Virensuche nach Viren durchsucht.

## Verwenden von Intego VirusBarrier X im Dock

Nach dem Starten von Intego VirusBarrier X wird das Programmsymbol im Dock von Mac OS X angezeigt.

Wenn Sie aufs Programmsymbol von Intego VirusBarrier X im Dock und anschließend auf die Schaltfläche "Im Dock halten" klicken, wird das Programmsymbol auch nach dem Beenden des Antivirusprogramms im Dock angezeigt.

Das Programmsymbol von Intego VirusBarrier X ist grün, wenn das Programm läuft, und rot, wenn es nicht läuft.

Sie können jederzeit Dateien, Ordner oder Datenträger aufs Programmsymbol von Intego VirusBarrier X ziehen, um diese Objekte auf Virenbefall zu prüfen. Wenn Intego VirusBarrier X noch nicht läuft, wird das Programm gestartet. In der Kugel für die funktionsabhängige Bedienung im Dock sehen Sie den Status der Virensuche.

Wenn Sie in den Voreinstellungen von Intego VirusBarrier X die Option "Programm verbergen" wählen, wird das Fenster des Antivirusprogramms nicht angezeigt. Alle Aktionen können aber in der Kugel im Dock verfolgt

werden. Weitere Informationen über die Voreinstellungen finden Sie im Abschnitt "Voreinstellungen von Intego VirusBarrier X" im Kapitel 6 dieses Benutzerhandbuchs.

# 5 - Funktionen von Intego VirusBarrier X

Intego VirusBarrier X ist ein leistungsfähiges und sehr einfach zu bedienendes Anwendungsprogramm zum Schutz Ihres Macintosh vor allen Arten von Computerviren. Das Antivirusprogramm arbeitet vollkommen unauffällig im Hintergrund und schützt Ihren Macintosh zu jeder Zeit.

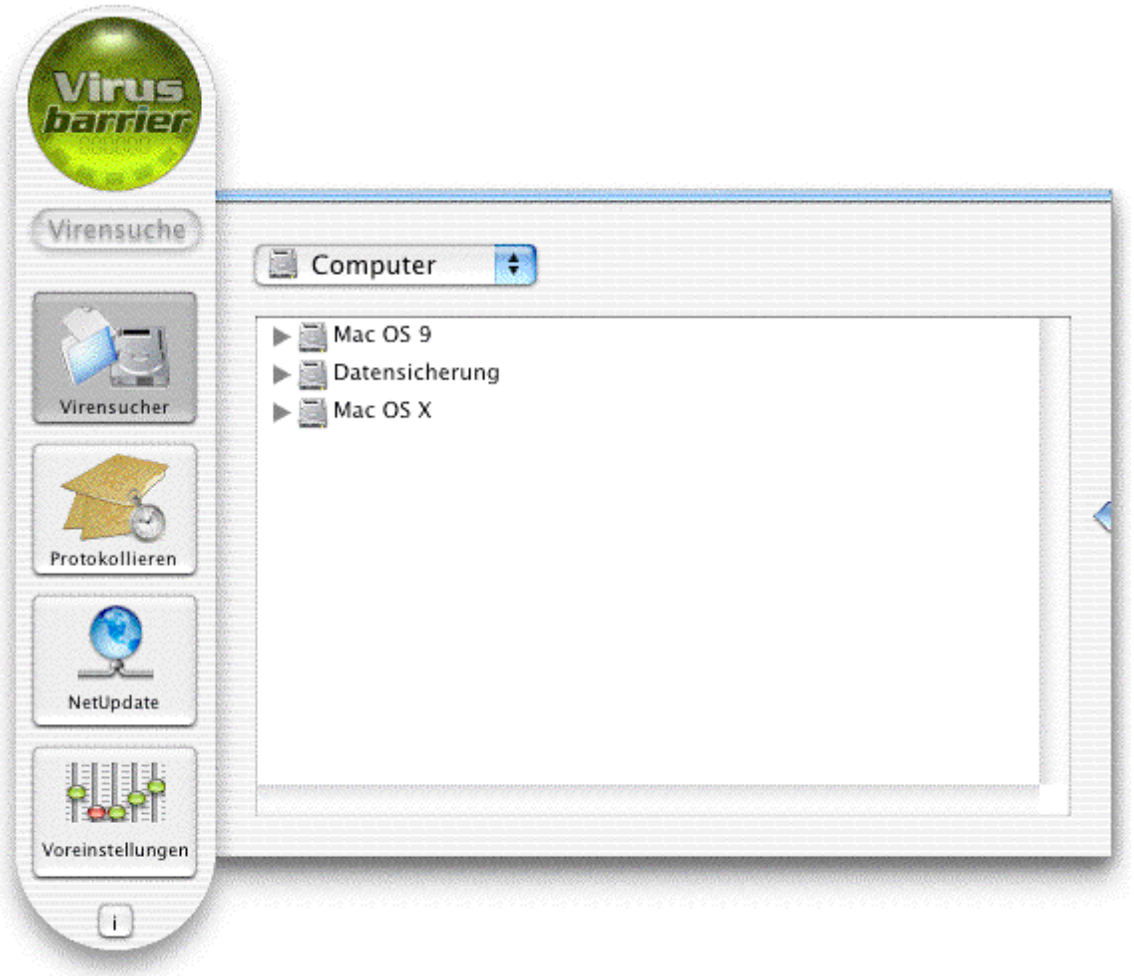
# Virensuche

Intego VirusBarrier X kann in unterschiedlichen Betriebsarten arbeiten. Das Antivirusprogramm überwacht Ihren Macintosh kontinuierlich auf verdächtige Aktivitäten, schützt ihn vor Virenbefall und prüft alle auswechselbaren Datenträger wie z.B. CD-ROMs und Zip-Disketten beim Anmelden auf Viren. Sie können eine Virensuche auf jedem Datenträger an Ihrem Macintosh oder im Netzwerk aber auch manuell starten.

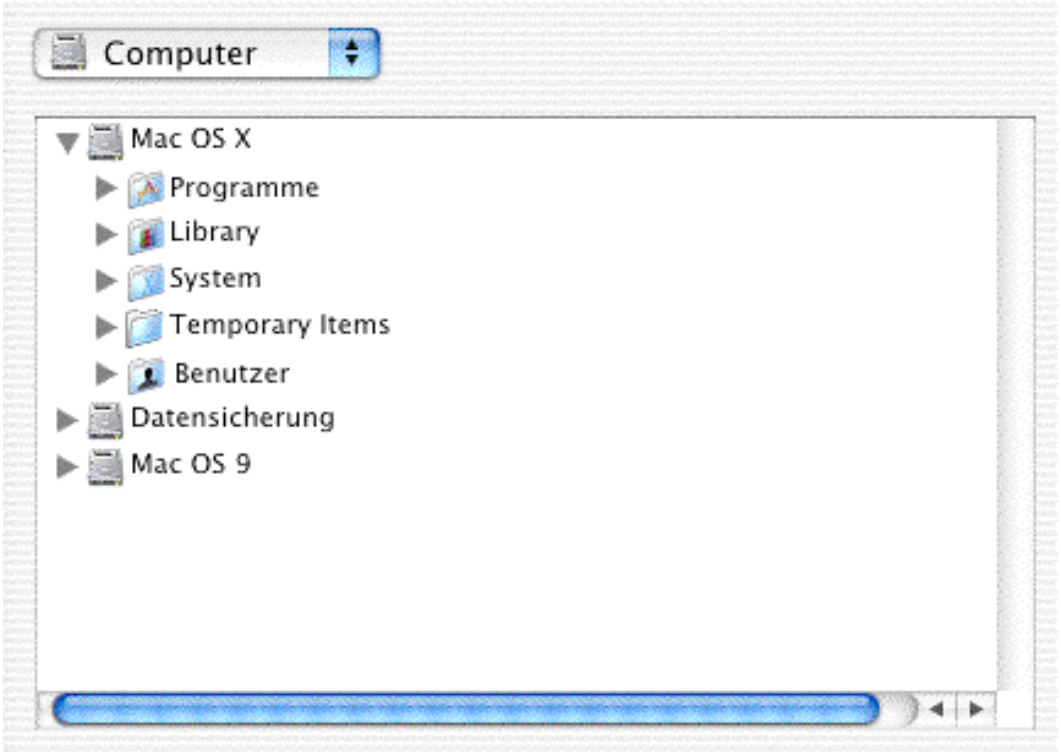
## Manuell gestartete Virensuche

Nach der Installation von Intego VirusBarrier X sollten Sie das Programm unbedingt eine Virensuche aller an Ihren Macintosh angeschlossenen Datenträger durchführen lassen. Hierdurch können Sie sicherstellen, dass Ihr Macintosh definitiv nicht mit einem Virus verseucht ist. Starten Sie die Virensuche unmittelbar nach dem Installieren von Intego VirusBarrier X.

Sie können jederzeit eine Virensuche starten, um einen Datenträger, einen Ordner oder eine Datei nach Viren zu durchsuchen. Starten Sie hierzu Intego VirusBarrier X und klicken Sie auf die Schaltfläche "Wählen".




Hierauf wird ein Schieber geöffnet, in dem alle momentan bei Ihrem Macintosh angemeldeten Datenträger angezeigt werden. In dieser Liste werden die Datenträger ähnlich wie im Finder dargestellt. Sie sehen hier Datenträger, Ordner und Dateien in hierarchischer Ordnung. Wenn Sie die Anzeige eines Datenträgers oder Ordners erweitern wollen, sodass Sie seinen Inhalt sehen können, müssen Sie nur aufs Dreieck links vom entsprechenden Symbol klicken. Um die Anzeige eines Datenträgers oder Ordners zu minimieren, müssen Sie nur auf dieses Dreieck klicken.


Computer
Mac OS X
Programme
Library
System
Temporary Items
Benutzer
Datensicherung
Mac OS 9

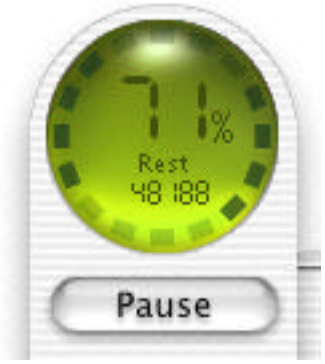
## Durchsuchen eines Datenträgers nach Viren

Wenn Sie einen Datenträger nach Viren durchsuchen wollen, müssen Sie nur auf sein Symbol doppelklicken oder es auswählen und auf die Schaltfläche "Virensuche" klicken. In der Kugel für die funktionsabhängige Bedienung sehen Sie nun, dass die Virensuche gestartet wurde. In der Kugel wird die Anzahl der bereits durchsuchten Dateien angezeigt.

Wenn Sie in den Voreinstellungen die Option "Restliche Dateien anzeigen" gewählt haben, zeigt Intego VirusBarrier X die Anzahl und den Prozentsatz der noch zu durchsuchenden Dateien an. Wenn Sie auf die Kugel klicken, wird auf

die Anzeige der bereits durchsuchten Dateien und des entsprechenden Prozentsatzes umgeschaltet.

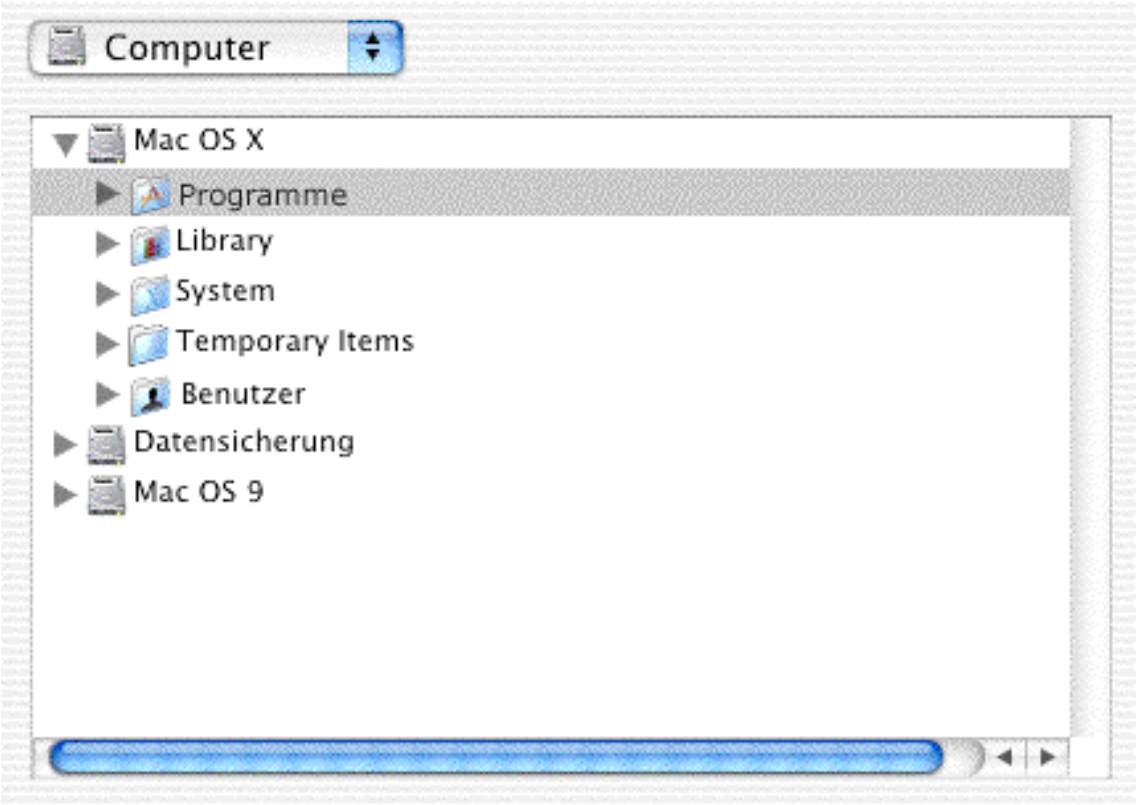
Sie können die Virensuche jederzeit stoppen, indem Sie auf die Schaltfläche "Stopp" klicken.




Wenn Sie die Virensuche vorübergehend anhalten wollen, müssen Sie die Umschalttaste in der Tastatureinheit Ihres Macintosh drücken. Hierauf ändert sich die Bezeichnung der Schaltfläche von "Stopp" in "Pause". Wenn Sie nun auf die Schaltfläche "Pause" klicken, wird die Virensuche vorübergehend angehalten.

Durch Klicken auf die gleiche Schaltfläche, die nun mit "Fortfahren" beschriftet ist, können Sie die Virensuche fortsetzen.

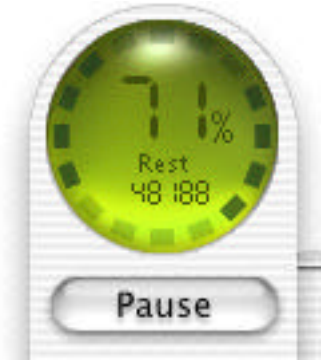
## Durchsuchen eines Ordners nach Viren



Wenn Sie einen Ordner auf einem Datenträger in oder an Ihrem Macintosh nach Viren durchsuchen wollen, müssen Sie aufs Dreieck links vom entsprechenden Datenträgersymbol klicken und dies so oft wiederholen, bis Sie das Symbol des gewünschten Ordners sehen können. Dopperlklicken Sie aufs Symbol des gewünschten Ordners oder klicken Sie einmal darauf und dann auf die Schaltfläche "Virensuche". In der Kugel für die funktionsabhängige Bedienung sehen Sie nun, dass die Virensuche gestartet wurde. In der Kugel wird die Anzahl der bereits durchsuchten Dateien angezeigt.

Wenn Sie in den Voreinstellungen die Option "Restliche Dateien anzeigen" gewählt haben, zeigt Intego VirusBarrier X die Anzahl und den Prozentsatz der noch zu durchsuchenden Dateien an. Wenn Sie auf die Kugel klicken, wird auf die Anzeige der bereits durchsuchten Dateien und des entsprechenden Prozentsatzes umgeschaltet.

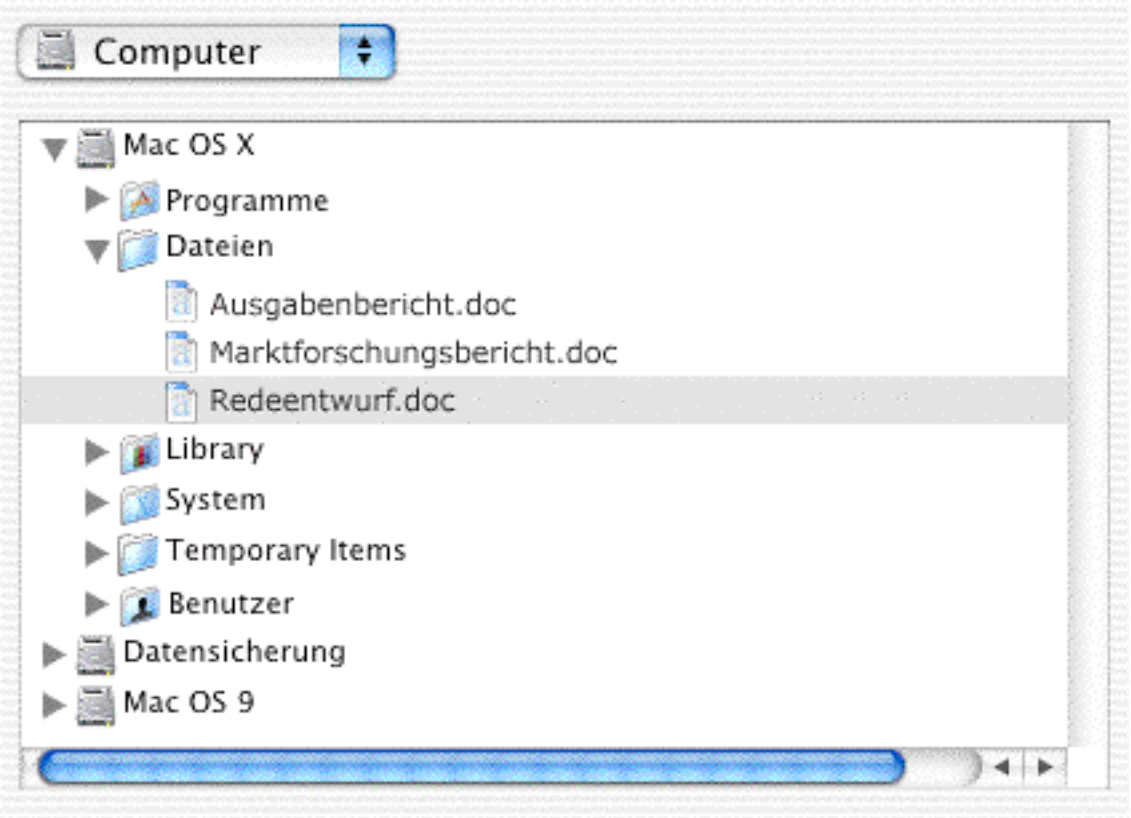
Sie können die Virensuche jederzeit stoppen, indem Sie auf die Schaltfläche "Stopp" klicken.




Wenn Sie die Virensuche vorübergehend anhalten wollen, müssen Sie die Umschalttaste in der Tastatureinheit Ihres Macintosh drücken. Hierauf ändert sich die Bezeichnung der Schaltfläche von "Stopp" in "Pause". Wenn Sie nun auf die Schaltfläche "Pause" klicken, wird die Virensuche vorübergehend angehalten.

Durch Klicken auf die gleiche Schaltfläche, die nun mit "Fortfahren" beschriftet ist, können Sie die Virensuche fortsetzen.

## Durchsuchen einer Datei nach Viren




Wenn Sie eine Datei auf einem Datenträger nach Viren durchsuchen wollen, der bei Ihrem Macintosh angemeldet ist, müssen Sie aufs Dreieck links vom entsprechenden Datenträgersymbol klicken und dies so oft wiederholen, bis Sie das Symbol der gewünschten Datei sehen können. Doppelklicken Sie aufs Symbol der gewünschten Datei oder klicken Sie einmal darauf und dann auf die Schaltfläche "Virensuche". In der Kugel für die funktionsabhängige Bedienung sehen Sie nun, dass die Virensuche gestartet wurde. Wenn Sie nur eine einzelne Datei prüfen, dauert dies unter Umständen nur Sekundenbruchteile, was Sie kaum sehen können.

## Virensuche mit Ziehen und Ablegen

Sie können jeden Datenträger oder Ordner, und auch jede Datei auf Viren durchsuchen, indem Sie ihn / sie einfach ins Fenster von Intego VirusBarrier X ziehen. Wenn Sie das jeweilige Symbol loslassen, wird das entsprechende Objekt auf die gleiche Weise wie beim manuellen Starten der Virensuche nach Viren durchsucht.

## Ergebnisse der Virensuche

Wenn Intego VirusBarrier X eine mit einem Virus infizierte Datei gefunden hat, wird automatisch das Protokollfenster geöffnet. In diesem Fenster sehen Sie eine Liste mit den Namen aller infizierten Dateien sowie den Namen der Viren, mit denen die Dateien infiziert sind. Wenn Sie Intego VirusBarrier X angewiesen haben, nur eine Virensuche und keine Reparatur durchzuführen, werden lediglich die Namen der infizierten Dateien und der Viren angezeigt. Wenn Sie Intego VirusBarrier X angewiesen haben, mit Viren infizierte Dateien automatisch zu reparieren, erscheinen in der Liste die Namen der reparierten Dateien und der entfernten Viren.

## Interpretation der Ergebnisse der Virensuche

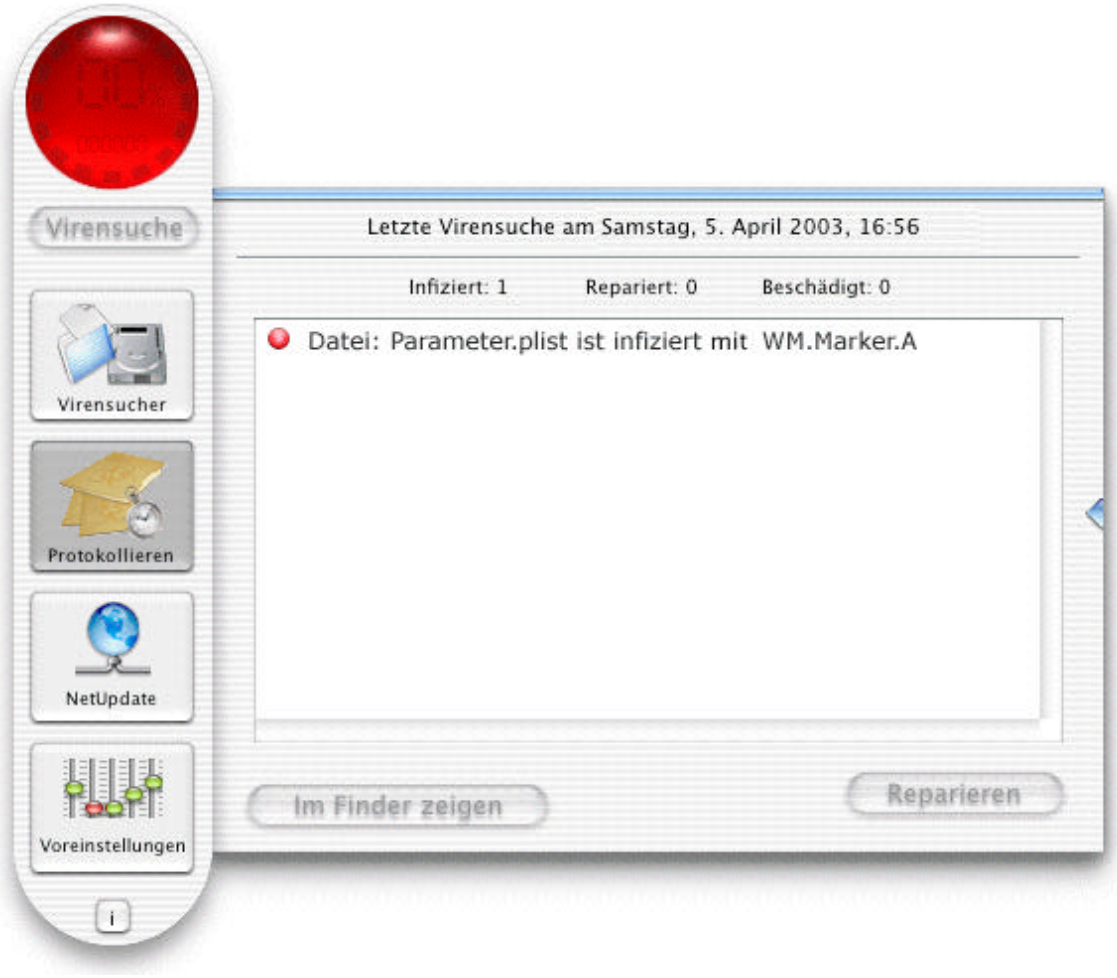
Intego VirusBarrier X informiert Sie darüber, ob mit bekannten Viren infizierte Dateien gefunden wurden. Das Antivirusprogramm alarmiert Sie auch, wenn es beschädigte Dateien erkannt hat.

## Mit Viren infizierte Dateien

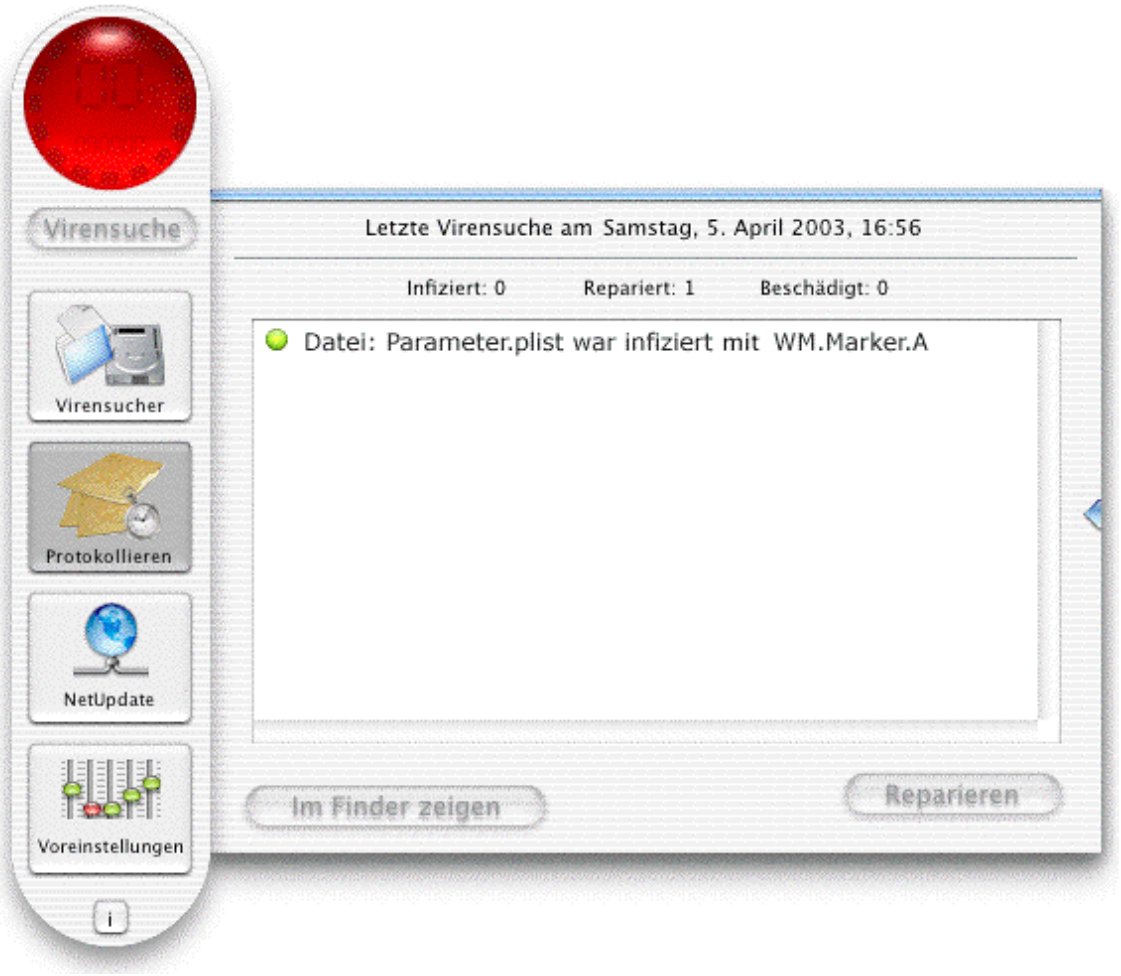
Wenn Intego VirusBarrier X eine mit einem Virus infizierte Datei gefunden hat, ändert sich die Farbe der Kugel für die funktionsabhängige Bedienung in Rot und der Protokollschieber wird geöffnet. Dieser Schieber wird nach dem Erkennen der ersten infizierten Datei geöffnet. Anschließend wird die Virensuche unter Umständen noch fortgesetzt. Intego VirusBarrier X alarmiert Sie gemäß den entsprechenden Voreinstellungen. Weitere Informationen über die Optionen für die Alarmierung finden Sie im Abschnitt "Voreinstellungen von Intego VirusBarrier X" im Kapitel 6 dieses Benutzerhandbuchs.

Welche Informationen im Protokollschieber angezeigt werden, hängt auch vom Virensuchmodus ab, den Sie in den Voreinstellungen ausgewählt haben. Sie

können Intego VirusBarrier X eine automatische Reparatur aller mit Viren infizierten Dateien durchführen lassen (Reparaturmodus) oder festlegen, dass Sie nur über infizierte oder beschädigte Dateien informiert werden (Virensuchmodus). Wenn Sie den Reparaturmodus gewählt haben, werden mit Viren infizierte Dateien nach Möglichkeit sofort repariert. Wenn Sie den Virensuchmodus gewählt haben, müssen Reparaturen manuell gestartet werden. Weitere Informationen über den Reparatur- und den Virensuchmodus finden Sie im Abschnitt "Voreinstellungen von Intego VirusBarrier X" im Kapitel 6 dieses Benutzerhandbuchs.



Wenn Sie den Virensuchmodus gewählt haben, werden im Protokollschieber die Namen der infizierten Dateien angezeigt. Wenn Sie eine oder mehrere Dateien reparieren wollen, müssen Sie diese auswählen und dann auf die Schaltfläche "Reparieren" an der Unterseite des Fenster klicken. Die Dateien werden nun repariert. Hierauf ändert sich die Anzeige im Protokollschieber entsprechend. Wenn Sie eine dieser Dateien im Finder sehen wollen, müssen Sie nur aufs Symbol oder den Namen der gewünschten Datei und dann auf die Schaltfläche "Im Finder zeigen" klicken.



## Beschädigte Dateien

Wenn Intego VirusBarrier X beschädigte Dateien erkannt hat, wird der Protokollschieber geöffnet. Dieser Schieber wird nach dem Erkennen der ersten beschädigten Datei geöffnet. Anschließend wird die Virensuche unter Umständen noch fortgesetzt. Intego VirusBarrier X alarmiert Sie gemäß den entsprechenden Voreinstellungen. Weitere Informationen über die Optionen für die Alarmierung finden Sie im Abschnitt "Voreinstellungen von Intego VirusBarrier X" im Kapitel 6 dieses Benutzerhandbuchs.

Eine beschädigte Datei enthält unter Umständen kein Virus, doch können Dateien von vielen Viren beschädigt werden, auch wenn sich das jeweilige Virus selbst nicht in diese Dateien kopiert hat. Diese Dateien können auch durch Festplattendefekte, Systemabstürze bei geöffneten Dateien usw. beschädigt werden. Beschädigte Dateien sollten möglichst durch einwandfreie Versionen ersetzt werden.

## Warnmeldungen

Eine Virensuche mit Intego VirusBarrier X kann zwar auch manuell gestartet werden, doch arbeitet das Antivirusprogramm normalerweise im Hintergrund. Wenn die Antivirussoftware eine mit einem Virus infizierte Datei erkennt, kann sie den Macintosh-Benutzer auf unterschiedliche Weise alarmieren.

Wenn Intego VirusBarrier X im Virensuchmodus eine infizierte Datei erkannt hat und somit keine automatische Reparatur durchführt, erscheint eine Warnmeldung auf dem Bildschirm des Macintosh.

Wenn Sie wollen, dass Intego VirusBarrier X die infizierte Datei repariert, müssen Sie auf die Schaltfläche "Reparieren" klicken. Wenn Sie dies nicht wollen, müssen Sie auf die Schaltfläche "Ignorieren". ACHTUNG: Dies kann gefährlich sein! Wählen Sie diese Option nur, wenn Sie auch wirklich wollen, dass infizierte Dateien nicht repariert werden.

Weitere Informationen über die Voreinstellungen in Bezug auf Warnmeldungen finden Sie im Abschnitt "Voreinstellungen von Intego VirusBarrier X" im Kapitel 6 dieses Benutzerhandbuchs.

# 6 - Einstellungen von Intego VirusBarrier X

# Voreinstellungen

Wenn Sie auf die Schaltfläche "Voreinstellungen" im Fenster von Intego VirusBarrier X klicken oder aus dem Menü die Option "Voreinstellungen..." wählen, stehen Ihnen mehrere Optionen zur Auswahl zur Verfügung. Auf der ersten Registerkarte können Sie die Optionen für den Virensuchmodus und auf der zweiten Registerkarte einige Optionen für die Alarmierung wählen.

## Virensuchmodus

Auf dieser Registerkarte können Sie festlegen, wie Intego VirusBarrier X nach Viren suchen soll. Ferner können Sie definieren, welche Informationen in der Kugel für die funktionsabhängige Bedienung angezeigt werden sollen.

### Modi

In diesem Abschnitt können Sie den Virensuchmodus wählen und festlegen, ob das Antivirusprogramm nach seinem Start sichtbar sein soll.

Sie können zwischen zwei Virensuchmodi wählen: Virensuche und Reparatur. Wenn Sie die Option "Nach Viren suchen" gewählt haben, gibt Intego VirusBarrier X eine Warnmeldung aus, sobald eine mit einem Virus infizierte Datei gefunden wurde. Infizierte Dateien werden jedoch nicht automatisch repariert. Wenn Intego VirusBarrier X während einer Virensuche eine mit einem Virus infizierte Datei erkennt, gibt das Programm eine Warnmeldung aus. Wenn Sie die Virensuche manuell gestartet haben, wird das Protokoll mit einer Liste der infizierten Dateien angezeigt. Wenn die infizierten Dateien repariert werden sollen, müssen Sie die Reparatur manuell starten. Dieser Modus eignet sich vor allem für den Fall, dass Ihr Macintosh mit einem

Netzwerk verbunden ist und Ihr Netzwerkverwalter mit Viren infizierte Dateien selbst untersuchen will.

Wählen Sie den gewünschten Virensuchmodus, indem Sie auf die entsprechende Schaltfläche klicken.
Wenn Sie das Kästchen "Programm verbergen" aktivieren, wird das Symbol von Intego VirusBarrier X nach dem Starten des Antivirusprogramms im Dock angezeigt. Das Programm selbst bleibt verborgen. Sie können Dateien, Ordner oder Datenträger nach Viren durchsuchen, indem Sie ihre Symbole aufs Symbol von Intego VirusBarrier X im Dock ziehen. Wenn Intego VirusBarrier X während der Virensuche eine mit einem Virus infizierte Datei erkennt, wird je nach den Einstellungen auf der Registerkarte "Warnmeldungen" eine Warnmeldung ausgegeben.

**Optionen**

Intego VirusBarrier X bietet Ihnen noch weitere Optionen zur Auswahl an.

**Turbomodus**

Wenn Sie das Kästchen "Turbomodus" aktivieren, läuft die Virensuche schneller ab. Beim erstmaligen Durchsuchen eines Datenträgers "merkt"

sich Intego VirusBarrier X, welche Dateien auf Viren durchsucht wurden. Wenn diese Dateien zwischenzeitlich nicht verändert wurden, so werden sie von Intego VirusBarrier X nicht durchsucht, sodass die Virensuche ca. 5- bis 40-mal schneller durchgeführt wird. Zwischenzeitlich veränderte oder neu erstellte Dateien werden jedoch nach Viren durchsucht. Nach jeder Aktualisierung der Virendefinitionen von Intego VirusBarrier X werden auch im Turbomodus alle Dateien durchsucht, um sicherzustellen, dass sie kein Virus enthalten, dessen Signatur erst in den neuen Virendefinitionen enthalten ist.

**Restliche Dateien anzeigen**

Wenn Sie diese Option gewählt haben, wird in der Kugel für die funktionsabhängige Bedienung von Intego VirusBarrier X nicht die Anzahl der bereits durchsuchten, sondern der noch zu durchsuchenden Dateien angezeigt.

**Komprimierte Dateien**

Wenn Sie die Option "Komprimierte Dateien" aktiviert haben, durchsucht Intego VirusBarrier X alle Dateien, die in StuffIt-Archiven enthalten sind (diese Archive enthalten komprimierte Dateien). Wenn komprimierte Dateien in einem StuffIt-Archiv nach Viren durchsucht werden, erscheint kurzzeitig ein Dialogfeld mit Informationen über infizierte und/oder beschädigte Dateien im StuffIt-Archiv auf dem Bildschirm Ihres Macintosh. Wenn ein StuffIt-Archiv mit Viren infizierte Dateien enthält, müssen Sie das Archiv erst einmal dekomprimieren.

Anschließend können Sie die dekomprimierten Dateien (oder Ordner) auf die Kugel von Intego VirusBarrier X ziehen und anschließend das StuffIt-Archiv mit den infizierten Dateien löschen.

**Unsichtbare Dateien anzeigen**

Wenn Sie dieses Kästchen aktiviert haben, werden unsichtbare Dateien im Browserschieber angezeigt.

**Klänge**

Intego VirusBarrier X kann Sie akustisch über vier verschiedene Situationen informieren:

- Virus erkannt
- Virus entfernt
- Beschädigte Datei
- Kein Virus erkannt

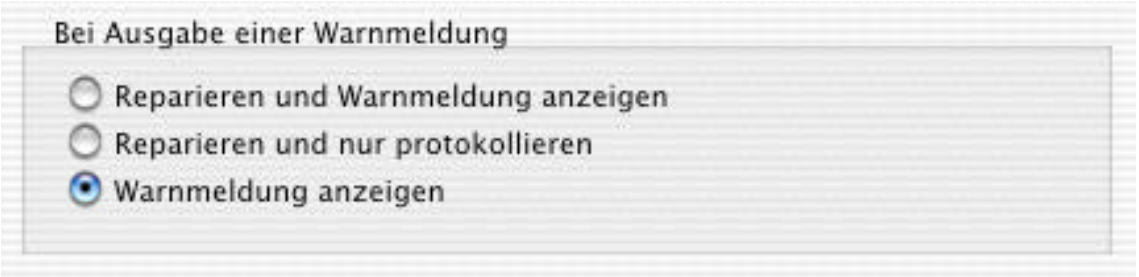
Wählen Sie die gewünschten Klänge. Hierbei handelt es sich um Ansagen mit synthetisierten Stimmen. Selbstverständlich können Sie auch andere auf Ihrem Macintosh installierte Klänge wählen; hierzu müssen Sie nur das Pop-Up-Fenster rechts vom jeweiligen Ereignis öffnen.

## Warnmeldungen

Auf dieser Registerkarte können Sie festlegen, wie Sie von Intego VirusBarrier X alarmiert werden wollen.

## Optionen für die Alarmierung

Intego VirusBarrier X kann Sie auf drei unterschiedliche Arten über mit einem Virus infizierte Dateien alarmieren, die während einer Virensuche im Hintergrund gefunden wurden.




**Reparieren und Warnmeldung anzeigen**

Wenn Sie diese Option gewählt haben, werden infizierte Dateien von Intego VirusBarrier X automatisch repariert. Gleichzeitig erscheint auf dem Bildschirm Ihres Macintosh eine Warnmeldung mit dem Namen der infizierten Datei und des gefundenen Virus.

**Reparieren und nur protokollieren**

Wenn Sie diese Option gewählt haben, werden infizierte Dateien von Intego VirusBarrier X automatisch repariert. Der Name der infizierten Datei und der Name des gefundenen Virus werden lediglich in die Protokolldatei geschrieben. Eine Warnmeldung wird nicht angezeigt. Wenn Sie mehr über die infizierten Dateien wissen wollen, müssen Sie das Protokoll einsehen.

**Warnmeldung anzeigen**

Wenn Sie diese Option gewählt haben, erscheint auf dem Bildschirm Ihres Macintosh eine Warnmeldung mit dem Namen der infizierten Datei und des gefundenen Virus. Gleichzeitig werden Sie gefragt, ob die infizierten Dateien repariert werden sollen.

## Optionen

**e-Mail-Mitteilung senden**

Wenn Sie dieses Kästchen aktiviert haben, sendet Intego VirusBarrier X innerhalb von 30 Sekunden automatisch eine e-Mail-Mitteilung an die ins Feld "Empfänger:" eingetragene e-Mail-Adresse. In die drei Felder müssen Sie den Namen des Absenders, die e-Mail-Adresse des Empfängers und den Namen des SMTP-Servers (für ausgehende e-Mail-Mitteilungen) eingegeben werden. Sie können diese e-Mail-Mitteilung auch an mehrere Adressaten versenden lassen. Die e-Mail-Adressen müssen in diesem Fall durch Kommas voneinander getrennt werden.

## NetUpdate

Wenn Sie auf die Schaltfläche "NetUpdate" klicken, wird der Schieber "NetUpdate" geöffnet. Dieser Schieber ermöglicht es Ihnen, eine Prüfung auf eine neue Version von Intego VirusBarrier X durchführen zu lassen. Hier sehen Sie auch Informationen wie das Datum der letzten Prüfung auf eine aktualisierte Version, die Nummer der derzeit auf Ihrem Macintosh installierten Version von Intego VirusBarrier X und das Ablaufdatum Ihres Abonnements auf Intego-Softwareaktualisierungen (sofern Ihr Abonnement gültig ist). Gleichzeitig mit dem Kauf von Intego VirusBarrier X erwerben Sie ein kostenloses Abonnement auf alle Aktualisierungen der Virendefinitionen über 1 Jahr.

Wenn Sie die Prüfung auf das Vorhandensein einer neuen Version von Intego VirusBarrier X auf dem Intego-Server manuell starten wollen, müssen Sie nur auf die Schaltfläche "Jetzt prüfen..." klicken. Hierauf wird Intego NetUpdate gestartet, stellt eine Verbindung mit dem Intego-Server her und prüft, ob dort eine neue Version von Intego VirusBarrier X oder neue Virendefinitionen vorhanden sind. Gleichzeitig mit dem Kauf von Intego VirusBarrier X erwerben Sie ein kostenloses Abonnement auf alle Aktualisierungen der Virendefinitionen über 1 Jahr.

Sie können NetUpdate konfigurieren, indem Sie das Zeitintervall für automatische Prüfungen auf aktualisierte Software festlegen. Hierzu steht Ihnen "NetUpdate Preferences" in den "Systemeinstellungen" zur Verfügung. Weitere Informationen über NetUpdate und die dazugehörigen Voreinstellungen finden Sie im NetUpdate-Benutzerhandbuch.

## Virenbeschreibung

Die zweite Registerkarte mit der Bezeichnung "Virenbeschreibung" enthält eine ausführliche Beschreibung sämtlicher bekannter Macintosh-Viren, vor denen Intego VirusBarrier X Ihren Macintosh schützt.

# Über Intego VirusBarrier X

Auf dieser Registerkarte finden Sie Informationen über Intego VirusBarrier X wie die Versionsnummer, Ihre Kundendienstnummer (die Sie benötigen, wenn Sie technische Kundenunterstützung anfordern), einen klickbaren URL (Universal Resource Locator = Adresse einer HTML-Seite im World Wide Web) der Intego-Website sowie die Postadresse und die Telefonnummer von Intego.

Wenn Sie Intego kontaktieren wollen, klicken Sie bitte auf den URL **Kontaktieren**. Hierauf öffnet Ihr e-Mail-Programm eine neue e-Mail-Mitteilung, in die bereits die e-Mail-Adresse von Intego und der Betreff "Mitteilung vom Kunden #" mit Ihrer Kundennummer eingetragen sind. Anschließend können Sie den Text Ihrer Mitteilung eingeben und diese absenden.

Wenn Sie Intego wegen technischer Kundenunterstützung kontaktieren wollen, klicken Sie bitte auf den URL **Kundenunterstützung**. Nun öffnet Ihr e-Mail-Programm eine neue e-Mail-Mitteilung, in die bereits die e-Mail-Adresse von Intego und der Betreff "Kundendienstanforderung vom Kunden #" mit Ihrer Kundennummer eingetragen sind. Anschließend können Sie den gewünschten Text eingeben und die e-Mail-Mitteilung absenden.

Wenn Sie auf den URL **Online registrieren** klicken, wird in Ihrem Internet-Browser die Seite für die Registrierung von Intego VirusBarrier X auf der Intego-Website geöffnet. Sie sollten Intego VirusBarrier X unbedingt bei Intego registrieren, damit Sie die neuesten Informationen über Intego VirusBarrier X und andere Intego-Produkte erhalten können.

Wenn Sie auf den URL **Website** klicken, öffnet Ihr Internet-Browser die Intego-Website.

# 7 - Diagnose

# Wenn Sie vermuten, dass Ihr Macintosh mit einem Virus infiziert ist

## Einige Symptome einer Infektion mit einem Virus

Die nachstehend beschriebenen Symptome deuten nicht in allen Fällen auf eine Infektion Ihres Macintosh mit einem Virus hin, doch sollten Sie durchaus misstrauisch sein:

- Auf dem Bildschirm Ihres Macintosh werden unerwartete Meldungen angezeigt.
- Ihr Macintosh stürzt immer wieder aus unerklärlichen Gründen ab.
- Auf Ihren Datenträgern (Festplatten usw.) finden aus unerklärlichen Gründen Lesevorgänge statt.
- Ihr Macintosh läuft ungewöhnlich langsam.
- Die freie Speicherkapazität auf Ihrer Festplatte hat sich erheblich verringert, ohne dass Sie viele neue Dateien angelegt haben.

Wenn Ihr Macintosh eines der vorgenannten Symptome aufweist, können Sie feststellen, ob das Problem von einem Virus oder einer anderen Software verursacht wird.

Zunächst sollten Sie das Dienstprogramm "Festplatten-Dienstprogramm" von Apple laufen lassen. Mit diesem Dienstprogramm können Sie Datenträger auf logische Fehler prüfen lassen. In den meisten Fälle können Sie diese Fehler mit dem Dienstprogramm "Festplatten-Dienstprogramm" reparieren. Sie finden

dieses Programm im Ordner "Dienstprogramme", der sich wiederum im Ordner "Programme" befindet. Wenn "Festplatten-Dienstprogramm" ein Problem erkennt, das es nicht beheben kann, benötigen Sie ein kommerziell verfügbares Datenrettungsprogramm.

Wenn das Problem auch mit einem derartigen Datenrettungsprogramm nicht beseitigt werden kann, sollten Sie herausfinden, welche Software Sie zuletzt installiert haben. Die meisten Computerprobleme werden durch Software verursacht. Wenn Sie also vor Kurzem neue Software installiert haben, sollten Sie diese versuchsweise entfernen und prüfen, ob das Problem weiterhin besteht.
Probleme können selbstverständlich auch von Hardware wie z.B. externen Festplattenlaufwerken, USB-Hardware, einem Drucker (bzw. dessen Treibersoftware) usw. verursacht werden. Trennen Sie diese Hardware versuchsweise von Ihrem Macintosh ab (bzw. entfernen Sie den Druckertreiber) und prüfen Sie, ob der Fehler nach wie vor auftritt.

Weitere Hilfe erhalten Sie unter Umständen auf der Website von Apple (www.apple.at, www.apple.ch oder www.apple.de), indem Sie dort auf die Registerkarte "Support" klicken.

Wenn Sie vermuten, dass Ihr Macintosh mit einem bisher noch unbekannten Virus infiziert ist, senden Sie bitte eine Kopie der entsprechenden Datei ans Intego Virus Monitoring Center. Weitere Informationen hierzu finden Sie im Abschnitt "Technische Kundenunterstützung" des Kapitels 8.

# Prinzipielle Vorsichtsmaßnahmen

Auch wenn Intego VirusBarrier X Ihren Macintosh kontinuierlich auf verdächtige Aktivitäten überwacht, sollten Sie einige wenige Vorsichtsmaßnahmen treffen, um sicherzustellen, dass Ihre Dateien nicht mit einem Virus infiziert werden können:

- Legen Sie regelmäßig eine Datensicherung Ihrer Dateien an. Verwenden Sie Intego Personal Backup X, um Datensicherungen automatisch durchzuführen.
- Legen Sie von Ihren wichtigsten Dateien mehrere Kopien an.
- Wenn Sie anderen Personen Ihre auswechselbaren, beschreibbaren Datenträger überlassen, sollten Sie deren Schreibschutz mit Hilfe der entsprechenden Schieber aktivieren.
- Setzen Sie Intego VirusBarrier X nur außer Betrieb, wenn dies zwingend notwendig ist. Intego VirusBarrier X muss im Gegensatz zu den meisten anderen Anwendungsprogrammen nicht außer Betrieb gesetzt werden, um neue Anwendungssoftware installieren zu können.
- Verwenden Sie niemals illegale Software. Dies ist nicht nur strafbar, sondern auch insofern gefährlich, als diese Software oft mit Viren verseucht ist, da sie von einem Computer zum anderen weitergegeben wird und deshalb leicht infiziert werden kann.
- Installieren Sie ausschließlich Software, deren Datenträger noch in die Originalverpackung eingeschweißt sind.
- Aktualisieren Sie Intego VirusBarrier X regelmäßig mit NetUpdate.

- Verwenden Sie zusätzlich zu Intego VirusBarrier X niemals ein anderes Antivirusprogramm, da es hierdurch zu Softwarekonflikten kommen kann.

# 8 - Technische Kundenunterstützung

Als registrierter Intego-Kunde erhalten Sie von Intego technische Kundenunterstützung.

## Per e-Mail:

support@intego.com

## Über die Intego-Website

www.intego.com

Wenn Sie vermutlich mit einem Virus infizierte Dateien ans Intego Virus Monitoring Center einsenden wollen, kontaktieren Sie dieses bitte vorher, indem Sie eine entsprechende e-Mail-Mitteilung an die e-Mail-Adresse sendvirus@intego.com schicken.

# 9 - Anhang

# Häufig verwendete Fachbegriffe

**Antivirusprogramm** - Ein Antivirusprogramm ist ein Programm, das einen Computer vor dem Befall durch Viren schützt, indem die an diesen Computer angeschlossenen Datenträger auf Viren durchsucht und eventuell mit Viren infizierte Dateien repariert werden. Zu diesem Zweck durchsucht das Antivirusprogramm jede Datei nach einem typischen Bitmuster ("Signatur"), das für einen der vielen existierenden Viren typisch ist.

**Archiv** - Unter Archiv wird bei einem Macintosh eine Datei verstanden, die mehrere - normalerweise komprimierte - Dateien enthält. Das Standardprogramm für die Datenkompression mit einem Macintosh ist das Programm StuffIt.

**Auswechselbarer Datenträger** - Jeder Datenträger, der aus dem zugehörigen Laufwerk herausgenommen werden kann. Typische auswechselbare Datenträger sind CD-ROMs, Disketten und Zip-Disketten.

**Code** - Computerprogramme bestehen aus Maschinencode, der durch Kompilieren aus dem von einem Programmierer geschriebenen Quellcode generiert wird. Da es sich bei Viren ebenfalls um Programme handelt, bestehen diese ebenfalls aus Maschinencode.

**Datenträger** - Prinzipiell ist ein Datenträger eine Festplatte oder ein auswechselbarer Massenspeicher. Das Betriebssystem betrachtet eine ganze Festplatte, einen Festplattenteilbereich, eine an einen Computer im Netzwerk angeschlossene Festplatte oder eine Diskette als Datenträger. Jeder Datenträger enthält einen aus mehreren speziellen Dateien bestehenden Dateikatalog, aus dem ersichtlich ist, wo die Dateien gespeichert sind.

**Falsche Viruswarnung** - Hierbei handelt es sich um Warnungen vor Viren, die es überhaupt nicht gibt. Per e-Mail werden schon seit Jahren viele falsche

Viruswarnungen verbreitet. In diesen e-Mail-Mitteilungen wird behauptet, dass das angebliche Virus bereits durch das Lesen einer e-Mail-Mitteilung aktiviert wird.

**Infiziert** - Wenn eine Datei mit einem Virus infiziert ist, bedeutet dies, dass sich das Virus selbst in die betroffene Datei kopiert hat. Bei diesem Virus kann es sich beispielsweise um ein Makrovirus handeln, das sich in eine Microsoft-Word-Datei kopiert hat. Es gibt auch Viren, die sich nur in Anwendungsprogramme kopieren.

**INIT** - Dies ist eine alternative Bezeichnung für eine Systemerweiterung. Dieser Begriff rührt daher, dass diese Dateien beim Starten eines Macintosh initialisiert werden.

**Makrobefehl** - Hierbei handelt es sich um ein kurzes Programm, das die in vielen Anwendungsprogrammen integrierten Möglichkeiten einer Makrobefehlssprache nutzt. Viele Anwendungsprogramme können Makrobefehle verarbeiten. Die Aufgabe von Makrobefehlen besteht darin, sich wiederholende Arbeitsschritte zu automatisieren. Unglücklicherweise können Makrobefehle auch Aktionen durchführen, die ein Computersystem beschädigen können. Es gibt Tausende von Makroviren, u.z. hauptsächlich für Microsoft Word und Microsoft Excel.

**Makrovirus** - Ein Virus, das auf das Vorhandensein einer Makrobefehlssprache angewiesen ist. Makroviren sind derzeit die gefährlichsten Viren für Macintosh-Computer. Die am häufigsten vorkommenden Makroviren gibt es für Microsoft Word und Microsoft Excel. Diese Makroviren können sowohl auf PCs mit dem Betriebssystem Windows als auch auf Macintosh-Computern Schäden anrichten, da diese beiden Anwendungsprogramme für beide Computerplattformen zur Verfügung stehen.

**Ressource** - Macintosh-Dateien bestehen eigentlich aus zwei Dateien: einem Ressourcenzweig ("ressource fork") und einem Datenzweig ("data fork"). Der Ressourcenzweig enthält beispielsweise Symbole, Programmcode usw. Einige Viren für den Macintosh kopieren sich selbst in die Ressourcenzweige von Dateien bzw. ändern oder beschädigen diese.

**Schreibtischdateien** - In diesen beiden Dateien werden Informationen über die Zuordnung von Symbolen zu Dateien und Anwendungsprogrammen gespeichert. Auf jedem Datenträger eines Macintosh befinden sich zwei Schreibtischdateien mit den Namen "Desktop DB" und "Desktop DF" (nur bei Mac OS 9). Die Schreibtischdateien werden von bestimmten älteren Macintosh-Viren attackiert. Die Schreibtischdateien werden vom Macintosh-Betriebssystem beim Anmelden eines Datenträgers gelesen.

**Starten** - Hierunter ist das Einschalten eines Macintosh und das Laden seines Betriebssystems zu verstehen.

**Systemerweiterung** - Systemerweiterungen (die auch als "INITs" bezeichnet werden) und Kontrollfelder sind Bestandteile des Macintosh-Betriebssystems. Sie erweitern das Betriebssystem um bestimmte Funktionen oder enthalten die Treibersoftware für bestimmte Hardware. Es gibt zwei Arten von Systemerweiterungen: Die einen werden während des Systemstarts geladen, und die anderen werden nur dann geladen, wenn sie vom Betriebssystem benötigt werden.

**Teilbereich** - Ein logischer Datenträger (Bereich auf einem physischen Datenträger wie z.B. einer Festplatte). Eine Festplatte kann in mehrere Teilbereiche untergliedert werden, die vom Betriebssystem wie separate Festplatten behandelt werden. Für ein Betriebssystem sind Teilbereiche separate (logische) Datenträger.

**Trojanische Pferd** - Ein Trojanisches Pferd (umgangssprachlich: "Trojaner") ist ein Programm, das zusätzlich zum eigentlichen Programmcode "bösartigen" Code enthält. Trojanische Pferde sind keine Viren, da sie sich nicht selbst vervielfältigen können. Manche Trojanischen Pferde enthalten jedoch Virencode, der in andere Dateien kopiert wird, nachdem das Trojanische Pferd gestartet wurde. Die Bezeichnung "Trojanisches Pferd" geht auf das riesige, innen hohle Pferd aus Holz zurück, das die alten Griechen laut ihrer Mythologie bauten und den Trojanern als eine Art Geschenk überließen, bevor sie sich an der Küste Trojas einschifften, um angeblich nach Hause zu segeln. In der darauffolgenden Nacht sprangen einige im Innern des Trojanischen Pferds verborgene griechische Krieger heraus und öffneten heimlich die Tore der Stadt, sodass Troja von den nun erneut heranstürmenden Griechen erobert werden konnte.

**Virus** - Ein "bösartiges" Computerprogramm, das sich selbst reproduzieren kann. Die meisten Viren sind bösartig und infizieren Dateien, indem sie sich selbst in die Dateien hineinkopieren. Die Viren verbreiten sich nach dem Öffnen der infizierten Dateien.

**Virusvariante** - Manche Viren kommen in unterschiedlichen Varianten vor. In dieser Hinsicht ähneln sie biologischen Viren, die schnell mutieren können.

**Wurm** - Ein Wurm ist ein Programm, das sich selbst über ein Netzwerk verbreitet. Obwohl die meisten Computerbenutzer glauben, ein Wurm sei nichts anderes als ein spezieller Virus, da auch Würmer Schäden anrichten können, funktionieren Würmer völlig anders als Viren. Würmer benötigen keine Wirtsdateien, um sich zu vervielfältigen.

# Virenbeschreibung

## ANTI

Das Virus ANTI trat zum ersten Mal in Frankreich, u.z. im Jahre 1989 auf. Die erste Variante dieses Virus war ANTI-A. Die zweite Variante namens ANTI-B wurde im Jahre 1990 entdeckt. Dieses Virus infizierte Anwendungsprogramme, aber keine System- und Datendateien. Das Virus ANTI kann nur Macintosh-Betriebssysteme bis zum System 6 befallen.

Dieses Virus, dessen Name von der eingebetteten Textzeichenfolge "ANTI" abgeleitet wurde, war ein relativ gefährliches Virus, da es Anwendungsprogramme beschädigte, die dann nicht mehr einwandfrei funktionieren konnten. Vom Virus ANTI infizierte Anwendungsprogramme können nicht repariert werden, sodass eine Neuinstallation dieser Anwendungsprogramme erforderlich ist. Diese Beschädigung der infizierten Anwendungsprogramme wurde höchstwahrscheinlich nicht vom Programmierer dieses Virus beabsichtigt, da sich das Virus lediglich selbst reproduziert und keine anderen Auswirkungen nach sich zieht.

Es sieht so aus, als sei die Variante ANTI-B noch vor der Variante ANTI-A entwickelt worden, da die Variante ANTI-A Programmcode enthält, der die Variante ANTI-B neutralisiert. Bis auf diesen Unterschied ähneln sich die beiden Varianten sehr.

**AutoStart-Würmer**

Im Mai 1985 wurde der erste Macintosh-Wurm entdeckt. Dieser Wurm verbreitete sich vor allem schnell über Südostasien, und danach über den gesamten Erdball. Der Wurm tritt in folgenden Varianten auf: AutoStart 9805-A, AutoStart 9805-B, AutoStart 9805-C, AutoStart 9805-D, AutoStart 9805-E und AutoStart 9805-F.

Dieser Wurm kann sich nur verbreiten, wenn beim betroffenen Macintosh die Funktion "Auto-Start" von QuickTime aktiviert ist und eine mit dem Wurm infizierte CD-ROM beim Betriebssystem angemeldet wird. Der Wurm kopiert sich selbst in Form mehrerer Dateien in den Ordner "Systemerweiterungen". Die Dateien haben folgende Bezeichnungen: "Desktop Print Spooler", "Desktop Print Spooler" oder "DELDesktop Print Spooler".

Der AutoStart-Wurm kann gravierende Schäden verursachen, indem er Dateien löscht und Daten zerstört. Die verschiedenen Varianten attackieren unterschiedliche Dateitypen. Beschädigte Dateien werden mit "Datenmüll" überschrieben und können weder repariert noch wiederhergestellt werden. Mit dem AutoStart-Wurm infizierte Macintosh-Computer fallen durch eine außergewöhnlich große Anzahl von Festplattenzugriffen in Zeitintervallen von 3, 6, 10 oder 30 Minuten auf. Unter Umständen ist im Menü "Programme" das Programm "Desktop Print Spooler" zu sehen.

**CDEF**

Das Virus CDEF wurde zuerst im Jahre 1990 in Ithaca im US-Bundesstaat New York entdeckt. Kurz danach wurde der Programmierer dieses Virus, von dem auch das Virus WDEF stammt, verhaftet. Der Name dieses Virus kommt daher, dass es eine CDEF-Ressource in den Macintosh-Schreibtischdateien verwendet, um sich zu reproduzieren. CDEF-Ressourcen sind normalerweise in bestimmten Anwendungsprogrammen und auch in der Systemdatei enthalten. Dies bedeutet, dass eine Datei, in der diese Ressource enthalten ist, nicht unbedingt mit dem Virus CDEF infiziert sein muss. Schreibtischdateien enthalten aber normalerweise keine CDEF-Ressource.

Das Virus CDEF infiziert ausschließlich Schreibtischdateien und verbreitet sich auf diese Weise von Datenträger zu Datenträger, da der Macintosh beim Anmelden eines Datenträgers die darauf befindlichen Schreibtischdateien ausliest. Dieses Virus wurde nicht programmiert, um Schäden zu verursachen, kann aber wie viele anderen Computerviren zu Fehlfunktionen eines Macintosh führen.

Im Jahre 1993 wurde eine zweite Variante des Virus CDEF entdeckt, die sich nur geringfügig von der ersten Variante unterscheidet.

**CODE-1**

Das Virus CODE-1 wurde zuerst im Jahre 1993 in den USA entdeckt. Es ist weitgehend unschädlich und infiziert lediglich die Systemdatei sowie Anwendungsprogramme. Wenn der mit diesem Virus infizierte Macintosh am

31. Oktober eines beliebigen Jahres gestartet wird, benennt das Virus den Systemdatenträger in "Trent Saburo" um. Dieses Virus kann sich zwar auf andere Macintosh-Computer verbreiten, verursacht aber nur Systemabstürze und beschädigt Anwendungsprogramme.

**CODE 252**

Das Virus CODE 252 wurde im Jahre 1992 in den USA entdeckt. Es infiziert sowohl die Systemdatei als auch Anwendungsprogramme. Wenn ein damit infizierter Macintosh zwischen dem 6. Juni und dem 31. Dezember eines beliebigen Jahres gestartet wird, erscheint folgende Meldung auf dem Bildschirm:

> You have a virus.
> Ha Ha Ha Ha Ha Ha Ha
> Now erasing all disks...
> Ha Ha Ha Ha Ha Ha Ha
> P.S. Have a nice day
> Ha Ha Ha Ha Ha Ha Ha
> (Click to continue...)

Trotz dieser Meldung löscht das Virus keine Dateien. Zu jeder anderen Zeit des Jahres (also vor dem 6. Juni) kopiert sich das Virus nur selbst aus Anwendungsprogrammen in die Systemdatei und von dort in andere Anwendungsprogramme. Unter System 7 gab es Systemabstürze und beschädigte Dateien; allerdings kopierte sich das Virus nicht in andere Anwendungsprogramme. Dieses unsachgemäß programmierte Virus

verursacht Systemabstürze und andere Schäden, da sein Programmcode mehrere Fehler enthält.

**CODE 9811**

Das Virus CODE 9811 wurde im November 1998 in Schweden entdeckt. Es verbirgt Anwendungsprogramme und ersetzt diese durch Dateien mit willkürlich gewählten Namen, die zudem "Datenmüll" enthalten. Mit einer Wahrscheinlichkeit von 25 % erscheint an Montagen die folgende Meldung auf dem Bildschirm des mit diesem Virus infizierten Macintosh: "You have been hacked by the Praetorians". Gleichzeitig erscheinen symbolisch gezeichnete Würmer auf dem Schreibtisch des Macintosh. Dieses Virus versucht auch, Antivirussoftware vom Systemdatenträger des infizierten Macintosh zu löschen.

**CODE 32767**

Dieses Virus wurde im Jahre 1997 entdeckt und ist sehr selten. Das Virus versucht einmal im Monat, Dokumente zu löschen.

**Flag**

Das Virus Flag (auch als WDEF-C bezeichnet) infiziert die Systemdatei und überschreibt die WDEF-Ressource mit der ID 0. Hierdurch können Probleme entstehen. Dieses Virus ist jedoch nicht sehr gefährlich. Es scheint heute nicht mehr in Umlauf zu sein.

**Frankie**

Das Virus Frankie stammt aus Deutschland, ist sehr selten und attackiert nur bestimmte Macintosh-Emulatoren auf Atari- und Amiga-Computer. Es sieht so aus, als solle sich dieses Virus gegen Anwender richten, die illegale Software einsetzen. Das Virus bewirkt, dass folgende Meldung auf dem Bildschirm des Computers erscheint: "Frankie says: No more piracy!". Der infizierte Atari-Computer stürzt dann ab. Macintosh-Computer werden von diesem Virus nicht infiziert. Allerdings verbreitet sich das Virus durch Infizieren von Anwendungsprogrammen, wobei Kopien davon einen Macintosh-Emulator auf einem Atari- oder Amiga-Computer infizieren können.

**Graphics Accelerator**

Siehe "SevenDust".

**INIT-M**

Das Virus INIT-M wurde im Jahre 1993 in den USA entdeckt. Es ist sehr gefährlich und wird an jedem 13. eines Monats aktiv, wenn dieser auch ein Freitag ist. Dieses Virus kann eine Vielzahl von Ordnern und Dateien beschädigen, indem es ihre Namen durch willkürlich gewählte Zeichenfolgen ersetzt. Dieses Virus ändert auch den Dateityp ("type") und die Kennung des Erzeugerprogramms ("creator") in willkürlich gewählte Zeichenfolgen aus 4 Zeichen, wodurch keine korrekte Zuordnung zu den Dateisymbolen möglich ist und die Dateien unbrauchbar werden. Dies kann nur rückgängig gemacht werden, indem der ursprüngliche Dateityp und die ursprüngliche Kennung des

Erzeugerprogramms wiederhergestellt werden. Ferner setzt dieses Virus das Erstellungsdatum und das Datum der letzten Änderung auf den 1. Januar 1904. In manchen Fällen löscht das Virus auch Dateien und / oder lässt Fenster fehlerhaft darstellen.

Das Virus INIT-M kann Dateien aller Typen infizieren und erzeugt im Ordner "Preferences" zusätzlich eine Datei namens "FSV Prefs".

**INIT 17**

Das Virus INIT 17 wurde im Jahre 1993 in Kanada entdeckt. Es infiziert die Systemdatei sowie Anwendungsprogramme. Wenn ein mit diesem Virus infizierter Macintosh am 31. Oktober 1993 nach 06:06:06 Uhr gestartet wurde, erschien auf dem Bildschirm die folgende Meldung: "From the depths of Cyberspace". Diese Meldung wurde nur ein einziges Mal angezeigt.

Dieses Virus war sehr fehlerhaft programmiert und verursachte auf einigen Macintosh-Computern mit dem Prozessor MC68000 Systemabstürze. Dies geschah eher unabsichtlich als absichtlich.

**INIT 29**

Dieses Virus wurde im Jahre 1988 und eine zweite Variante im Jahre 1994 entdeckt. Die beiden Varianten werden gelegentlich als INIT 29 A und INIT 29 B bezeichnet.

Bei INIT 29 handelt es sich um ein sehr gefährliches Virus. Es infiziert System-, Anwendungsprogramm- und Dokumentendateien, die allerdings keine anderen Dateien infizieren können.

Dieses Virus verbreitet sich lediglich und richtet keinen eigentlichen Schaden an. Nach dem Einlegen einer schreibgeschützten Diskette ins Diskettenlaufwerk bewirkt das Virus die Anzeige der folgenden Meldung:

> The disk "xxxx" needs minor repairs.
> Do you want to repair it?

Infizierte Macintosh-Computer reagieren auf dieses Virus gelegentlich mit Systemabstürzen, Druckproblemen usw.

**INIT 1984**

Das Virus INIT 1984 wurde im Jahre 1992 in den Niederlanden und in den USA entdeckt. Wie viele anderen Viren wird auch dieses Virus nur aktiv, wenn der infizierte Macintosh am 13. eines Monats gestartet wird, wenn dieser auch ein Freitag ist. Wie das Virus INIT-M kann dieses Virus eine Vielzahl von Ordnern und Dateien beschädigen, indem es ihre Namen durch willkürlich gewählte Zeichenfolgen ersetzt. Dieses Virus ändert auch den Dateityp ("type") und die Kennung des Erzeugerprogramms ("creator") in willkürlich gewählte Zeichenfolgen aus 4 Zeichen, wodurch keine korrekte Zuordnung zu den Dateisymbolen möglich ist und die Dateien unbrauchbar werden. Dies kann nur rückgängig gemacht werden, indem der ursprüngliche Dateityp und die ursprüngliche Kennung des Erzeugerprogramms wiederhergestellt werden.

Das Erstellungsdatum und das letzte Änderungsdatum dieser Dateien werden auf den 1. Januar 1904 gesetzt.

Dieses Virus infiziert ausschließlich Systemerweiterungen ("INITs"). Das Virus verbreitet sich nicht so schnell wie Viren, die Anwendungsprogrammen attackieren, da Systemerweiterungen nicht so häufig wie Anwendungsprogramme von einem Macintosh-Benutzer an andere weitergegeben werden.

**INIT 9403**

Dieses Virus wird auch als SysX bezeichnet. Es wurde im Jahre 1994 in Italien entdeckt. Derzeit werden damit nur Macintosh-Computer infiziert, auf denen eine italienische Version des Macintosh-Betriebssystems läuft. Dieses Virus ist sehr gefährlich: es löscht Dateien und versucht, aktuell beim Betriebssystem angemeldete Datenträger zu löschen. Es sieht so aus, als sei dieses Virus zusammen mit illegaler Software verbreitet worden. Es infiziert den Finder sowie bestimmte Kompressions- und Archivierungsprogramme.

**Makroviren**

Heutzutage stellen Makroviren die gefährlichsten Computerviren für Macintosh-Benutzer dar.

Das erste echte Makrovirus hieß "Concept"; es attackierte Microsoft-Word-Dateien. Varianten dieses Makrovirus folgten Schlag auf Schlag, da die Virenprogrammierer aufgrund der Verwendung des

Textverarbeitungsprogramms Microsoft Word durch Millionen von Computerbenutzern die Möglichkeit sahen, großen Schaden anzurichten. Später wurden auch Makroviren speziell für Microsoft Excel programmiert. Innerhalb von nur 5 Jahren nach dem Auftauchen des ersten Makrovirus wurden Tausende dieser Computerviren programmiert.

Die große, von Makroviren ausgehende Gefahr besteht darin, dass es sich um die ersten Computerviren für unterschiedliche Computerplattformen handelt. Über viele Jahre hinweg konnten sich die Benutzer von Macintosh-Computern relativ gut vor Computerviren geschützt fühlen, da es für den Macintosh nur ein paar Dutzend Viren gab, während es Windows-Benutzer mit Abertausenden von Viren zu tun hatten. Doch nun, seit dem Auftauchen der ersten Makroviren, sehen sich auch Macintosh-Benutzer mit dem Problem der Computerviren konfrontiert.

Die meisten Makroviren für Microsoft Word verwenden Befehle wie AutoOpen, AutoClose, AutoExec und AutoExit. Hierbei handelt es sich um Befehle, die ausgeführt werden, wenn eine bestimmte Aktion stattfindet. Diese vier Aktionen werden beim Arbeiten mit jeder Datei ausgeführt. Wenn ein Makrovirus beispielsweise so programmiert wäre, dass es sich nur dann in eine andere Datei kopiert, wenn ein bestimmter Menübefehl aufgerufen wird, würde es sich mit geringerer Geschwindigkeit verbreiten.

Deshalb treten die meisten Makroviren bereits beim Öffnen einer Datei in Aktion, um sich dann in die gleichzeitig geöffnete Vorlage zu kopieren. Diese Vorlage wird nicht eigens vom Benutzer, sondern automatisch im Hintergrund

geöffnet. Vorlagen enthalten bestimmte Anpassungsinformationen und auch zulässige Makrobefehle, die vom Benutzer in der Vorlage gespeichert wurden.

Das häufigste Makrovirus für Microsoft Word kopiert sich selbst in die momentan aktive Vorlage, ändert einige Menüoptionen, sodass die Vorlage nicht mehr geändert werden kann, ändert den Dateityp (wodurch die zugeordneten Symbole geändert werden, sodass die Dateien als Vorlagen erscheinen) und kopiert nun das Makrovirus aus der infizierten Vorlage in alle zukünftig geöffneten oder neu erstellten Dateien. Dieses Makrovirus kann gelöscht werden, indem die aktive Vorlagendatei und alle infizierten Dateien gelöscht werden.

Andere Makroviren können noch weitaus gefährlicher werden. Sie können Ihre Dateien beschädigen oder löschen, bestimmte Funktionen des entsprechenden Anwendungsprogramms unzugänglich machen, und vieles mehr. Makroviren sind plattformunabhängig, d.h. sie sind sowohl für PCs mit dem Betriebssystem Windows als auch für Macintosh-Computer gefährlich.

**MacMag**

Das Virus MacMag ist ein Beispiel für etwas, das zwar in guter Absicht getan wurde, aber negative Auswirkungen zur Folge hat. Dieses Virus wurde fürs Macintosh-Magazin MacMag programmiert und sollte auf den Bildschirmen der damit infizierten Computern eine Friedensbotschaft darstellen, sofern der jeweilige Macintosh am 2. März 1988 gestartet wurde. Anschließend sollte sich das Virus selbst löschen. Das Virus MacMag war ursprünglich Bestandteil eines HyperCard-Stapels namens "New Apple Products" (der also selbst ein

Trojanisches Pferd war) und verbreitete sich durch Infizieren der Systemdatei. Das Virus MacMag findet man heute höchstwahrscheinlich nur noch auf alten CD-ROMs usw.

**MBDF**

Dieses Virus wurde dank der internen Virensuchfunktion von Claris-Anwendungsprogrammen im Jahre 1992 in Wales, Großbritannien, entdeckt. Das Virus MBDF wurde ursprünglich über die Spiele "10 Tile Puzzle" und "Obnoxious Tetris" sowie ein Trojanisches Pferd namens "Tetricycle" verbreitet. Im Gegensatz zu den meisten anderen Fällen konnten die Urheber des Virus MBDF, zwei US-amerikanische College-Studenten, dingfest gemacht und überführt werden.

Dieses Virus infiziert sowohl Anwendungsprogramme als auch die Systemdatei, indem eine MBDF-Ressource mit der ID 0 kopiert wird. Wenn die Systemdatei jedoch eine Ressource mit diesem Namen enthält, wird sie nicht verändert.

Obwohl dieses Virus eigentlich nicht schädlich ist, kann es die Systemdatei beschädigen, sodass diese vom Benutzer neu installiert werden muss. Das Virus verursacht auch Probleme mit der Menüdarstellung. Dieses Virus existiert in zwei verschiedenen, aber kaum unterschiedlichen Varianten: MBDF A und MBDF B.

**MDEF**

Dieses Virus gibt es in vier Varianten: MDEF-A, MDEF-B, MDEF-C und MDEF-D. Die Variante MDEF-A wird gelegentlich als "Garfield" und die Variante MDEF-B als "Top Cat" bezeichnet. Diese beiden Varianten wurden in den Jahren 1990 und 1991 in Ithaca im US-Bundesstaat New York entdeckt. Kurz danach wurde der Programmierer dieses Virus, von dem auch das Virus CDEF stammt, verhaftet.

Der Name des Virus rührt daher, dass sich dieses durch Kopieren einer MDEF-Ressource reproduziert. MDEF-Ressourcen sind normalerweise in bestimmten Anwendungsprogrammen und auch in der Systemdatei enthalten. Dies bedeutet, dass eine Datei, in der diese Ressource enthalten ist, nicht unbedingt mit dem Virus MDEF infiziert sein muss.

Das Virus MDEF attackiert Anwendungsprogramme, die Systemdatei, Dokumentendateien und die Schreibtischdateien. Dieses Virus kann beträchtlichen Schaden anrichten, obwohl dies von seinem Programmierer höchstwahrscheinlich nicht beabsichtigt war. Das Virus kann manche Anwendungsprogramme und andere Dateien beschädigen.

**MDEF 666**

Siehe "SevenDust".

**MDEF 9806**

Siehe "SevenDust".

**MDEF 999**

Siehe "SevenDust".

**noir**

Das Virus "noir" wurde im Jahre 1987 in Europa entdeckt. Es gibt die beiden Varianten "noir A" und "noir B". Dieses Virus ist auch unter mehreren anderen Namen (AIDS, Fuck, Hpat, Jude, MEV# und nFlu) bekannt.

Dieses Virus wurde ohne böse Absichten programmiert und vervielfältigt sich durch Infizieren der Systemdatei und von Anwendungsprogrammen. Das Virus lässt ein akustischen Signal installieren. Wenn auf dem infizierten Macintosh das Sprachausgabesystem MacInTalk installiert ist, ertönt die Ansage "Don't panic". Diese Effekte treten beim Starten des Betriebssystems, aber mit unterschiedlicher Häufigkeit auf.

**Scores**

Das Virus Scores ist auch unter anderen Bezeichnungen (Eric, Vult, NASA und San Jose Flu) bekannt. Es wurde im Jahre 1988 in den USA entdeckt. Scores wurde von seinem Urheber höchstwahrscheinlich dazu programmiert, um das Verhalten von Computerviren zu untersuchen. Allerdings verbreitete sich das

Virus sehr schnell. Das Virus erzeugt zwei unsichtbare Dateien mit den Namen "Scores" und "Desktop_", infiziert die Systemdatei und beschädigt die Notizblock- und die Albumdatei, indem es deren Symbolzuordnung verändert. Anschließend infiziert das Virus gerade laufende Anwendungsprogramme. Allerdings kann es nicht jedes Anwendungsprogramm infizieren. Das Virus Scores kann willkürlich auftretende Systemabstürze und Druckprobleme verursachen.

**SevenDust**

Das Virus SevenDust existiert in mehreren Varianten von A bis G. Dieses Virus ist auch unter den Bezeichnungen MDEF 9806 und MDEF 666 bekannt. Diese Viren verbreiten sich über MDEF-, MENU- oder WIND-Ressourcen und eine Systemerweiterung. SevenDust E, eine auch als "Graphics Accelerator" bekannte Variante, wurde im Jahre 1998 in einem Trojanischen Pferd entdeckt.

Diese Viren können Anwendungsprogramme, die Systemdatei und Kontrollfelder infizieren. Sie versuchen, alle Dateien auf dem Systemdatenträger zu löschen, bei denen es sich nicht um Anwendungsprogramme handelt. Dies findet nur am 6. und 12. jedes Monats zwischen 06:00 und 07:00 Uhr statt.

Die Variante "SevenDust F" wurde über ein Trojanisches Pferd namens "ExtensionConflict" verbreitet. Von dieser Varianten gibt es fünf weitere Subvarianten, die sich nur über andere Systemerweiterungen reproduzieren.

**SysX**

Siehe INIT 9403.

**T4**

Das Virus T4 wurde im Jahre 1992 entdeckt. Es wurde über das Spiel "GoMoku" in den Versionen 2.0 und 2.1 verbreitet, die auf mehrere FTP-Server hochgeladen worden waren. Dieses Virus infiziert Anwendungsprogramme und den Finder, und versucht, die Systemdatei zu verändern. Das Virus maskiert sich auch als das kostenlose Antivirusprogramm "Disinfectant", um andere Antivirusprogramme zu überlisten.

Das Virus T4 kann die Systemdatei irreparabel beschädigen und willkürlich auftretende Systemabstürze verursachen. In manchen Fällen kann ein mit diesem Virus infizierter Macintosh nicht mehr gestartet werden.

Im Jahre 1997 wurde eine andere Variante mit der Bezeichnung T4-D gefunden. Diese Variante löscht Dateien im Systemordner, aber nicht die Systemdatei. Diese Variante verbreitet sich von einem Anwendungsprogramm zum anderen, indem sich das Virus selbst in die CODE-Ressource des jeweiligen Anwendungsprogramms einbettet.

**WDEF**

Das Virus WDEF wurde im Jahre 1989 in Belgien entdeckt. Seinen Namen hat es von der WDEF-Ressource in den Schreibtischdateien. Die beiden Varianten

WDEF A und WDEF B, die sich durch Infizieren der Schreibtischdateien (diese werden beim Anmelden jedes Datenträgers beim Betriebssystem gelesen) reproduzieren, verbreiten sich ziemlich schnell. Hierzu ist es nicht einmal nötig, ein Anwendungsprogramm zu starten.

Das Virus WDEF richtet keinen eigentlichen Schaden an, doch wurde es fehlerhaft programmiert, sodass es Systemabstürze und fehlerhafte Darstellung von Schriften verursachen kann.

**ZUC**

Das Virus ZUC wurde zuerst im Jahre 1990 entdeckt. Seinen Namen erhielt es von seinem Entdecker, Don Ernesto Zucchini. Von diesem Virus existieren drei Varianten: ZUC A, ZUC B und ZUC C. Sie infizieren ausschließlich Anwendungsprogramme und können sich sogar vervielfältigen, wenn keine Anwendungsprogramme laufen. Diese Varianten verursachen lediglich eine fehlerhafte Darstellung des Mauszeigers. Andere Schäden sind nicht bekannt.